SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

IT'S MINE!

WHY THE US INTELLIGENCE COMMUNITY DOES NOT SHARE INFORMATION

by

Andrew W. Green, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Everett Carl Dolman

Maxwell Air Force Base, Alabama

July 2005

APPROVAL

The undersigned certify that this thesis meets masters-level standards of research, argumentation, and expression.

_____

Everett Carl Dolman, PhD (Date)

_____

Lieutenant Colonel Gerald S. Gorman (Date)

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

ABOUT THE AUTHOR

Major Andrew W. Green was commissioned through the Reserve Officer Training Corps at Embry-Riddle Aeronautical University in 1990. After completing Air Force Intelligence Applications Officer training as a Distinguished Graduate, he was assigned to Onizuka AFB, where he served as the Special Security Officer for the 2nd Satellite Tracking Group. From there he went to Osan AB, Republic of Korea where he was a Watch Officer and later the Chief of the Electronic Threat Evaluation Branch. Major Green was next assigned to the 7th Airborne Command and Control Squadron where he worked as an Airborne Intelligence Officer on the Airborne Battlefield Command and Control Center aircraft. He next went to the Pentagon where he worked as an analyst, an Executive Officer, and as a Chief of Staff of the Air Force Daily Intelligence Briefer. Following his Pentagon tour, Major Green served as the Air Force representative to the White House Situation Room. Major Green has a Bachelor of Science degree in Aeronautical Engineering from Embry-Riddle Aeronautical University and a Master of Science in Management from Troy State University.

Contents

Preface

As a career Intelligence Officer I have a vested interest in how well the intelligence community (IC) functions. Following the four most recent investigations of the performance of the IC, I noticed a recurring theme within the findings – that the intelligence community tends to not share information and that this lack of sharing subsequently causes breakdowns in the IC's performance.

This led me to begin to explore the reason why the IC doesn't like to share intelligence information. As I explored this I found three possible explanations for the IC not sharing information. First that the organizational structure of the IC prevents effective sharing, second that the nature of the information itself prevents sharing, and third that the way the IC attempts to work collectively on a problem inhibits sharing.

The answer I found seems to indicate that all three contribute to the lack sharing; however, the organizational and informational problems seem to be the biggest factors in the IC not sharing intelligence information.

As with all projects like this the number of people that deserve to be thanked is greater than my supply of paper. First I would like to thank my adviser Dr. Everett Dolman who took time out of his schedule to help me finish this project. More important however is my wife Tonia and daughter Madison, who stuck by me as I toiled to complete this thesis. All I can say to both of them is that mere thanks is not enough to show my appreciation for all that I put you through.

Abstract

Although the US government has access to vast amounts of information, the system for processing and using that information is weak. The fact that the intelligence community (IC) shows a propensity to not share information among its many agencies is not a revolution. The problem has dogged the IC since its post-World War II inception. The vital issue, then, is not that a problem exists, but that the problem persists. Specifically, "why does the IC not share information?"

There is, undoubtedly, a myriad of plausible and valid explanations for every instance in which a single individual or agency in the intelligence community (IC) did not share information with another individual or agency. A cursory review of examples where a lack of timely information sharing contributed to intelligence failure, however, suggests three broad categories of theory are likely candidates for a more comprehensive explanation of intelligence sharing deficiency. These are organizational theories of bureaucratic inefficiency, theories of the evolving nature of information and power, and theories of collective *in*action.

Each of the theories expanded upon above provide a viable explanation as to why the IC is not willing to share intelligence information. Each accepts the premise that organizations exist in order to achieve the needs of the organization in the most efficient and effective means possible. However, each finds inherent structural limitations that prevent the organization from achieving goal optimization. Although all three theories are compelling in their own right, the interaction of the three provides a compelling rationale for why the IC should be *expected* to operate suboptimally—if not dysfunctionally—in its work.

Chapter One

Problem, Relevance, and Method

During its investigation into the events that surrounded the Al Qaida terrorist attacks of 11 September, 2001, the 9/11 Commission found that the biggest impediment to all-source analysis is "the human or systemic resistance to sharing information."[1] It pointed out that although the US government has access to vast amounts of information, the system for processing and using that information is weak. That the intelligence community (IC) shows a propensity to not share information among its many agencies is not a revolution. The problem has dogged the IC since its post-World War II inception. The vital issue, then, is not that a problem exists, but that the problem persists. Specifically, "why does the IC not share information?"

While there are perceived advantages *and* disadvantages to sharing information among its many disparate member organizations, so as to facilitate the IC's ability to collaborate or conduct group analysis, it seems that the benefits outweigh the shortcomings—an assessment based on Congress' recent passage of the National Security Intelligence Reform Act of 2004, which calls for a new Director of National Intelligence to increase collaboration across the community. The overriding belief is that the greater the amount of information available to enlighten the problem, the more likely it becomes the IC will arrive at an accurate assessment.

The Argument:

There are several perceived advantages to increased information sharing that dominate the debate. First is the notion that a broader level of expertise can be applied to a given problem. The IC consists of fifteen separate agencies, each of which has a different focus and diverse areas of proficiency. Second, by applying the widest possible range of expertise to a problem, the core belief is that a consensus view or solution will

1. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report.* Official Government Edition (Washington D.C.: U.S. Government Printing Office, 2004), 416. Hereafter cited as the *9/11 Commission Report.*

emerge that is more applicable to the problem than might occur if one or two agencies were to do the same analysis in isolation. Policymakers are well aware of the differing expertise in the IC, and they are likely to be more comfortable with an IC assessment that is unanimous (or nearly so). Consensus removes some of the risk the policymaker may have faced had the IC disagreed.

Information sharing is not a panacea, however. There are also numerous perceived *dis*advantages to the IC collaborating and conducting group analysis. One of the most vexing to collaborative analysis is the potential loss of competing or marginal views that in retrospect (as with the previous comment on the potential disadvantages of too much information) often tend to be right. In a collaborative environment the dissenting voice tends to be overwhelmed as the group works to maintain its cohesiveness. This leads to the possible loss of valid *competitive* analysis. In a rational economic, or market analysis model of optimizing information use, competing analysis over time tends to provide the most cost-efficient and accurate information over time. To carry the analogy further, collaborative analysis would have an effect equivalent to a monopolistic cartel, artificially impinging on cost-value and efficiency.

Another disadvantage to sharing intelligence information and conducting collaborative analysis is the very real danger of what Irving Janis has described as *groupthink*. Groupthink describes a mode of behavior individuals engage in when the desire to maintain group cohesiveness overrides their willingness to seriously consider alternative options or modes of thought.[2] Adding to the problem of consensus-seeking when valid options have not yet been adequately presented to the group is the desire of many individuals to have the "winning" argument by bringing the group around to his or her point of view. This creates a confounding dynamic whenever unanimous participation or agreement is required of the group—any single holdout has extraordinary bargaining power.[3]

A third perceived disadvantage, related to but significantly different than the groupthink phenomena, is the down side of *satisficing*. This is the process by which a

---

2. Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, Second Edition (Boston, MA: Houghton Mifflin Company, 1982), 9.

3. Mancur Olson, The Logic of Collective Action: Public Goods and the Theory of Groups (Cambridge, MA: Harvard University Press, 1971), 41.

group of individuals select a course of action that meets the most (or neglects the fewest) goals of the many individual positions rather than seeking the one best course of action. In relation to the IC, satisficing can be thought of as analysis of the most common denominator. Said another way, it is analysis that the group as a whole is willing to accept, rather than determining which is the best analysis, based on the information at hand.

Although the perception that the advantages to sharing intelligence information outweighs the disadvantages it does not provide any insight as to why the IC doesn't share. Instead the perception has become the impetus for change within the IC. However for the proposed change to be effective it should, in theory, address the reason why the IC doesn't share information. Only by answering this question will we be able to determine if the proposed changes to the IC will facilitate increased information sharing throughout the intelligence community.

Method

This thesis represents an attempt to answer the question, "Why does the intelligence community not share information?" The approach used is comparative inquiry.[4] First, I describe three of the dominant theoretical explanations for non-cooperation in groups, highlighting specific hypotheses that apply to the context of the IC, to provide a logical basis in support of the argument. Then, applying evidence from the brief history of the IC, I compare the observed behavior to the theoretical framework in order to draw relevant recommendations for consideration.

When John Stuart Mill first described the logic of comparative inquiry, he stipulated that its value would only be in the simplest of hard sciences—physics at its lowest levels—due to the inability to control for a significant number of variables.[5] Nonetheless, social scientists have adapted his methods by bundling extraneous characteristics to isolate and factor out non-intervening variables, limit the effects of irrelevant or marginally significant intervening variables, and magnify the impact of

4. The comparative inquiry approach is explained in Adam Przeworski and Henry Teune's book *The Logic of Comparative Social Inquir*y (Melbourne, FL: Krieger, 1982).

5. John Stuart Mill, System of Logic Rational and Deductive: Being a Connected View of the Principles of Evidence and the Methods of Scientific Investigation (London: Longman's, 1864). See Book III, Chapter VIII].

significant intervening variables.[6] Two methods were described by Mill: (1) The *Method of Agreement* is comparing together different instances in which a phenomenon occurs, and (2) the *Method of Difference,* or comparing instances in which the phenomenon does occur, with instances in other respects similar in which it does not.[7] In the first method, if *a, b,* and *c* are different in every way but one, then that sole similarity is the cause of *x*—the phenomenon under study. In the latter method, if *a, b,* and *c* are alike in every way but one, then the lone difference is the cause, or a necessary variable, of *x*. The most informative means of using these methods is to alternate them, that is, finding instances in which there appear to be similarities, noting then the total differences (for the purposes of bundling extraneous variables), then looking again for similarities.

Such is the comparative method, with Skocpol's admonitions, used here. Three periods are selected first for their similarities; these are US national intelligence organization and perceived failures in the Cold War, the post-Cold War, and in the first part of the twenty-first century. Then these instances are examined for their meaningful differences (thus bundling out the plethora of similarities that have little or no effect). Following that examination, remaining similarities are linked to theoretical explanations to harness their explanatory power. With this method, applicable recommendations based on theories of organization, information, and collective action theory are isolated.

Limitations and Assumptions:

Although much, if not most, of the intelligence community work is classified, no classified sources or information was accessed in the conceptual, research, or written phases of this thesis. The intent was to make this thesis as available as possible while still applying some academic rigor to the problem. Because of its unclassified nature however, the examples of behavior that I was able to use were ones that are readily available in an open forum. Much of this publicly available information is found in the investigative reports of previous intelligence community failures vice successes. This lack of information made it difficult to find both a positive and negative test case for all

6. Theda Skocpol, States and Social Revolutions: A Comparative Analysis of France, Russia, and China (Cambridge: University Press, 1979).

7. Mill, *System of Logic*, Book III, Chapter VIII, Section VII.

assessments of the theoretical approaches, i.e. those in which the IC *did* share information that resulted in either an intelligence success or failure.

It is absolutely critical to highlight one of the key assumptions in this thesis—Congress and the President have decided that it is in the nation's best interest to have the IC move in the direction of increased information sharing. This move began with the creation of the Director of National Intelligence. Nowhere in this thesis is an argument for or against the decision to do so, although both advantages and disadvantages of information sharing are discussed when explaining the logic of specific theoretical perspectives relevant to the analysis. Hence, I will only provide analysis-supported policy recommendations that aid increasing or facilitating information sharing within the overarching framework of the changes to the IC that are already underway.

Chapter Outline

Chapter two of this thesis provides the theoretical framework for the argument. It starts with a description of how governmental organizations act and interact, and continues with an explanation of some of the relevant issues that arise as organizations try to satisfy both the needs of the organization and of the individuals *within* the organization. Included is a discussion of Graham Allison and Philip Zelikow's influential *Essence of Decision.* Using Allison and Zelikows's governmental action as organizational output (or Model II behavior) as starting point, an overview of groupthink, information, and collective action theories complete the justification for the analytical framework.

Chapter three describes the historical foundations of the IC and also contains a discussion of the evolution of the IC during the Cold War. Included are some of the organizational changes that took place during this time. The chapter begins with a discussion of the events that led up to the creation of the intelligence community—the Japanese attack on Pearl Harbor—and then moves into a discussion of the events surrounding the creation of the IC via the National Security Act of 1947. Following is a discussion of some of the investigations that examined the performance of the IC as it related to its ability to support national foreign policy. The chapter concludes with a

discussion of the collapse of the Soviet Union—which the IC failed to anticipate, thus bounding the period with a pair of historically significant intelligence failures.

Chapter four includes an examination of the period immediately following the end of the Cold War and continues through to contemporary intelligence practices. As with the Cold War chapter, this period is delimited by two intelligence breakdowns: the failure to predict the Iraqi invasion of Kuwait in 1990, and the failure of the IC to accurately assess Iraq's weapons of mass destruction programs. The latter failure directly influenced the US-led invasion of Iraq in 2003. In between these bracketing events were several perceived missteps, including IC's failure to anticipate and warn about India's test of five nuclear warheads in May 1998. This chapter is focused on these three events, and in doing so provides within the theoretical framework proposed an argument as to why the three failures occurred.

Chapter five contains an examination of what may be considered the final straw in the intelligence community's poor performance: the IC's failure to anticipate the terrorist attacks against the United States on 11 September 2001. This failure led to the first investigations concerning the performance of the intelligence community in the twenty-first century, and provided the impetus for the most significant reorganization of the IC since its inception in 1947. As such, this chapter relies almost exclusively on the two investigations that occurred as a result of this attack. Again, by examining the events that contributed to this failure against the theoretical framework provided, we may gain some insight into how these kinds of failures may be prevented in the future.

Finally, in chapter six, I provide some recommendations that the Director of National Intelligence, and the IC as a whole, may wish to consider as the process of transforming the IC's functions and responsibilities moves forward. I close with some overall conclusions that hopefully will provide some additional insights into how the IC functions.

Chapter Two

Why the IC Doesn't Share Information: Theoretical Perspectives

There is, undoubtedly, a myriad of plausible and valid explanations for every instance in which a single individual or agency in the intelligence community (IC) did not share information with another individual or agency. A cursory review of examples where a lack of timely information sharing contributed to intelligence failure, however, suggests three broad categories of theory are likely candidates for a more comprehensive explanation of intelligence sharing deficiency. These are organizational theories of bureaucratic inefficiency, theories of the evolving nature of information and power, and theories of collective *in*action. The first highlights the manner in which organizations are developed and how different organizations interact with each other. The second emphasizes the nature of information itself, focusing on the traditional role of classified information common to the IC. The final perspective complements the first two, forming the basis for drawing together all three in a more complete theoretical explanation of information sharing.

As such, this chapter comprises the theoretical framework with which evidentiary cases are then examined. By subjecting the projected outcomes of theoretical explanations to instances in which a lack of intelligence sharing was credited at least in part for an intelligence failure, a pattern of interactions can be discerned. These patterns will do more than reinforce the validity of the theoretical perspectives under study; they will form the basis for a set of policy recommendations should decision makers wish to increase the prospect of IC information sharing in the future.

Organizational Behavior as the Catalyst for Not Sharing

Organizations are social units (or human groupings) deliberately constructed and reconstructed to achieve specific goals.[1] This definition provides insight into two areas of applicable interest. First, organizations are comprised of individuals, each with his or

1. Talcott Parsons, *Structure and Process in Modern Societies* (Glencoe, IL: The Free Press, 1960), 17.

her own needs. Second, the organization exists for a specific reason, without which the organization might be expected to fall apart or disband. These critical animating features of organizations and social groups will be evident in all three theoretical perspectives under investigation, and are in fact the associative basis for selecting them as analytical models for this study.

Goals or interests are the crux of meaningful difference between organizations and individuals. Organizational goals provide the organization with orientation and legitimacy. These, in turn, help to justify its existence.[2] With this in mind, it is important to note that there are different synonyms for the relatively neutral word organization. One of these is bureaucracy, which tends to have very negative connotations. Another synonym is community, which tends to have a more positive association but might be less accurate in its description, especially when applied to the intelligence community of the United States.

As much as the intelligence community may want to be a true community, it is saddled with many of the trappings of a classic bureaucracy.[3] The IC consists of 15 different agencies.[4] Most of the agencies within the IC are part of another agency that resides within the Executive branch of the US government. For example, the State Department's Bureau of Intelligence and Research (State/INR) is a member of the intelligence community, yet it is part of the overall Department of State, and its employees are bound by the rules and regulations of the State Department. The only exception to this is the Central Intelligence Agency (CIA). The CIA in its entirety is considered part of the intelligence community. Each of the agencies within the IC can be considered a bureaucratic organization based on the definition provided by Max Weber in

2. Amitai Etzioni, *Modern Organizations* (Englewood Cliffs, N.J.: Prentice-Hall Inc., 1964), 5.

3. *Webster's College Dictionary* 2000, Revised Edition, defines Community as "a social, religious, occupational, or other group sharing common characteristics or interests: *the business community*."

4. The members of the US intelligence community are the Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Reconnaissance Office (NRO), the National Geospatial Intelligence Agency (NGA), the Defense Intelligence Agency (DIA), the intelligence organizations of each of the armed services (including the US Coast Guard), the Federal Bureau of Investigation (FBI), the Bureau of Intelligence and Research of the State Department (State/INR), the Department of the Treasury, the Department of Energy, and the Department of Homeland Security. It should be noted that the new Director of National Intelligence and the organization that is created to support this office is also a member of the US intelligence community.

his foundational text, *The Theory of Social and Economic Organization*. According to Weber, bureaucracies display:

(1) A continuous organization bounded by rules.
(2) A specified sphere of competence. This involves (a) a sphere of obligations to perform functions which has been marked off as part of a systematic division of labor (b) the provision of the incumbent with the necessary authority to carry out these functions (c) the necessary means of compulsion are clearly defined and their use is subject to definite conditions.
(3) The organization of offices follows the principle of hierarchy.
(4) The rules with regulate the conduct of an office may be technical rules or norms.
(5) It is a matter of principle that the members of the administrative staff should be completely separated from ownership of the means of production.
(6) Administrative acts, decisions, and rules are formulated and recorded in writing, even in cases where oral discussion is the rule or is even mandatory.
(7) Legal authority can be exercised in a wide variety of ways.[5]

Each of these applies to every agency of the IC, reinforcing the conceptual view of the IC as a conglomerate of bureaucratic organizations.

According to leading organizational theorist Amitai Etzioni, organizations have their own needs. They can be expected to work towards fulfilling these needs as they work to reach their goals or desired state of affairs.[6] Accordingly, it is assumed that organizations are constructed *to be effective and efficient* in attaining organizational goals or desired state of affairs. However, Etzioni also points out that "probably the most important structural dilemma is the inevitable strain imposed on the organization by the use of knowledge. All social units use knowledge, but organizations use more knowledge more systematically that do other social units. Moreover most knowledge is created in organizations and passed from generation to generation – i.e. preserved – by organizations."[7] The challenge for IC agencies then comes in determining how they can create and use the knowledge that they have while at the same time protecting this knowledge to ensure that the organization is fulfilling its most vital need—the need to exist.

In order for an organization to be truly efficient and effective, it needs to meet not only the goals of the organization, but also the needs of the personnel within the

5. Max Weber, *The Theory of Social and Economic Organization*, Talcott Parsons (ed.); translated by A.M. Henderson and Talcott Parsons (New York, N.Y.: Oxford University Press, 1947), 329-332.
6. Etzioni, *Organizations*, 6.
7. Ibid., 75.

organization. These needs, however, are typically set and monitored *outside* the organization. The "trend in modern democratic societies, especially in the United States, has been to try to find a new balance between the organizational demands placed on participants and their personal and extra-organizational needs."[8]

Relationships can occur across level, as in the personal to organizational one just described, as well as across systems, in this case between individuals (discussed more directly later on) or between organizations.[9] Relations among organizations are also to some extent regulated by the state, which provides laws, administrative agencies, courts, and regulatory commissions that set the limits within which each of the IC organizations act and interact. There are four ways to view the interaction between agencies:

1) Laissez-faire ideology associate with the tradition liberal conception of the state. In this model the state is expected to refrain from interfering in the relationships among organizations unless absolutely necessary, and this is mainly to avoid major public injury.
2) The State actively regulates a much larger variety of organizational interaction.
3) A system of indicative planning in which the state provides a list of economic goals that are likely to gain support in the future is necessary to ensure continuity.
4) Totalistic planned system in which most of the organizations are subordinate directly to the state and receive specific orders from superior state organizations.[10]

The IC has tended to follow a pattern closer to the top of this list than the bottom, and perceived failures in information sharing are pressing current designs toward the bottom, a not necessarily desirable yet unavoidable restructuring.[11]

Another useful way to view the IC organizationally is found in Graham Allison and Philip Zelikow's *Essence of Decision*.[12] Although Allison and Zelikow provide three different models to explain how government decision-making occurs, the appropriate one here is their second, or model II, explanation of bureaucratic behavior. Because the IC is comprised of a large number of agencies, most of which belong to another agency within

---

8. Ibid., 115.

9. Adam Prjeworski and Henry Teune, *The Logic of Comparative Social Inquiry* (Melbourne, FL: Krieger, 1982), 6.

10. Etzioni, *Organizations*, 110.

11. *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-458, 108th Cong. (17 December 2004), 1.

12. Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, Second Edition (New York, Addison-Wesley Educational Publishers, Inc., 1999), 2-7.

the executive branch of government, Allison and Zelikow's model II construct, governmental action as organizational output, provides the most applicable framework for analyzing the IC's unwillingness to share information.

Model II views governments as consisting of large organizations each of which has different responsibilities. This allows the government to meet a wide spectrum of needs for its citizens and respond to a wide variety of problems.[13] The US intelligence community is a subset of the broader government, organized in a similar fashion in that it consists of large organizations, among which primary responsibility for tasks is divided. Ideally, each organization attends to a special set of problems, and acts in quasi-independence on these problems. With each organizational positive, however, there is a negative. In this case, few of the meaningful problems organizations deal with fall completely within the domain of one single organization. The predicament becomes one of organizational *in*efficiency, stemming from issue and authority deconfliction.

Model II relies on the "logic of appropriateness" as defined by March and Simon to explain how organizations make decisions.[14] With logic of appropriateness, actions are chosen "by recognizing a situation as being of a familiar, frequently encountered, type, and matching the recognized situation to a set of rules...the logic of appropriateness is linked to conceptions of experience, roles, and intuition, and expert knowledge. It deals with calculation mainly as a means of retrieving experience preserved in the organization's files or individual memories."[15] When working with a representative of model II behavior, one is most likely to find an individual who will rely on the organization's routines to deal with a problem rather than that individual analyzing the situation and thinking about what would be sensible in the particular situation.

There are five key points that need to be considered when examining Model II organizational behavior.

1) Organizations are collections of human beings arranged systematically for harmonious or unified action.
2) Organizations create capabilities for achieving humanly-chosen purposes and performing tasks that would otherwise be impossible.

---

13. Ibid., 143.

14. "Introduction to the Second Edition," in James G. March and Herbert A. Simon, *Organizations*, Second Edition (Cambridge: Blackwell Publishers, 1993), 8. See also James G. March, *A Primer on Decision Making: How Decisions Happen* (New York: Free Press, 1994), viii.

15. Ibid.

3) Existing organizations and their existing programs and routines constrain behavior in the next case: namely, they address it already oriented toward doing whatever they do.
4) Organizational culture emerges to shape the behavior of individuals within the organization in ways that conform with informal as well as formal norms.
5) Organizations are thus less analogous to individuals than to a technology or bundle of technologies.[16]

Thus, Model II behavioral explanations reveal that organizational priorities will tend to shape organizational implementation of solutions. For instance, "organizations will tend to emphasize, in practice, the objectives most congruent to their special capacities and to the hierarchies of beliefs in the organization's culture."[17] Therefore, if an organization is presented with conflicting goals, the organization will satisfy one, while deferring or neglecting the other.

Model II behavior also shows that governmental organizations have limited control over the organization of production; limited control over their goals; and that their output comes in a form that makes it difficult to assess success or failure – except in very specific instances.[18] This lack of control is often the result of a paradox regarding governmental action requiring the decentralization of responsibility and power, which conflicts directly with the requirement for coordination among agencies.[19] This curious and diametric situation, one that must look self-defeating to outsiders, is that the "American public bureaucracy is not designed to be effective."[20]

A third way to examine the workings of the intelligence community, following discussions of the dynamic between organizational and individual goals and Allison and Zelikow's model II rationale, is by looking at it as a result of *how* large organizations or groups function. Here the intelligence community can be viewed as a group of groups.[21] Often times the IC works to build a consensus position, and in doing so can be infected by and suffer from the decision-making flaws of *any* of its individual member groups. A more insidious problem is the structural output of both individuals in groups and/or of

16. Allison and Zelikow, *Essence of Decision*, 145.
17. Ibid.,177.
18. James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989), 113-136, and 156-171.
19. Allison and Zelikow, *Essence of Decision*, 172.
20. Terry M. Moe, "The Politics of Bureaucratic Structure," in John Chubb and Paul Peterson (eds.), *Can the Government Govern?* (Washington, DC; Brookings Institution, 1989), 267.
21. This is the essence of Plurality Theory in political science. See Robert Dahl, *Who Governs?* (New Haven: Yale University Press, 1961) for its foundational theory.

groups interacting identified by Irving Janus as *groupthink*, "a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members' striving for unanimity override their motivation to realistically appraise alternative courses of action. Groupthink refers to a deterioration of mental efficiency, reality testing, and moral judgments that results from in-group pressures."[22] Some of the more specific defects that are likely to occur because of group decision-making include:

1) Group discussions are limited to a few alternative courses of action.
2) Group does not survey the objectives to be fulfilled and the values implicated by the choice.
3) Group fails to reexamine the course of action initially preferred by the majority of the members from standpoint of nonobvious risks and drawbacks that had not been considered when it was originally evaluated.
4) Members neglect courses of action initially evaluated as unsatisfactory by the majority of the group.
5) Members make little or no attempt to obtain information from experts who can supply sound estimates of losses and gains to be expected from alternative courses of action.
6) Selective bias is shown in the way the group reacts to factual information and relevant judgments from experts, the mass media, and outside critics.
7) Members spend little time deliberating about how the chosen policy might be hindered by bureaucratic inertia, sabotaged by political opponents, or temporarily derailed by the common accidents that happen to the best of well-laid plans.[23]

Other problems with group decision-making include the social pressure to conform, and the conflicting secondary goal of some individual's desire to win the argument within the group.[24]

Although the hazards of groupthink are real, there nonetheless remains a number of long standing perceived advantages to group problem solving. Some of these include: the greater sum of total knowledge and information that the group has; the greater number of approaches to the problem that the group is likely to take; the fact that participation in solving the problem increases acceptance of the final solution; and that there will be better comprehension of the final analysis as a result of group

22. Janis, *Groupthink*, 9.
23. Ibid., 10.
24. Norman R. F. Maier, "Assets and Liabilities in Group Problem Solving: The Need for an Integrative Approach," in Walter E. Natemeyer (ed.), *Classics of Organizational Behavior* (Oak Park, IL: Moore Publishing Company, Inc., 1978), 142.

participation.[25] All of these benefits apply to an IC that is looking for thoughtful solutions to problems that have traditionally been contained within highly compartmented organizations. Opening up the process of analysis to include larger numbers of analysts from a wider scope of experience and expertise levels, it is hoped, will improve the probability of reaching a consensus that is more balanced and useful to the decision maker.

In addition, there are aspects of group decision-making that can be either an advantage or a disadvantage, depending on the group. For example, the group discussion may lead to an agreement that can serve to either create animosity between the group members or result in an innovative solution.[26] Socialization can occur among members that will either promote further integration and cooperation or could cause fractionalization and limit cooperation in associated areas.

Ultimately, properly selected groups have the potential to contend with and solve problems that far exceed the capacities of even a superior individual. It is this lure of the possible that causes groups to continuously form and reform in the bureaucracy, despite the now well-known hazards. The goal is "for a...group to establish a problem solving process that capitalizes upon the total pool of information and provides for a great interstimulation of ideas without any loss of innovative creativity due to social constraints."[27] However, whether a group will work effectively on an organizational task and at the same time become satisfying to its members depends in part on the group composition. For effective work to occur, the group must share at least some basic values and agree on a medium for communication.[28]

What these organizational theories reveal is that an organization is most likely to share information as long as the organization itself can benefit from the exchange. Meeting the goals and needs of the organization *and* its members is the paramount concern of the organization. Even in the case of groupthink, in which individual

---

25. Norman R. F. Maier, "Assets and Liabilities in Group Problem Solving: The Need for an Integrative Approach," in Natemeyer, *Classics of Organizational Behavior*, 140-141

26. L.R. Hoffman, "Conditions for Creative Problem Solving," *Journal of Psychology* 52 (1961), 429-444.

27. J.W. Thibaut and H.H. Kelley, *The Social Psychology of Groups* (New York: Wiley, 1961), 268.

28. Edgar H. Shchien, "Groups and Intergroup Relationships," in Natemeyer, *Classics of Organizational Behavior*, 155.

members of the organizations that make up the IC are expected to be representing their respective agencies, the willingness of the members to share information is likely to be tied to the interests of the organization that the individual is representing. While all of these theories present optimizing solutions to the problem of individual and group organization, each is dependent on details of context for its utility. Following a discussion of IC examples in the following chapters, in which organizational factors are highlighted, specific recommendations are offered in the final chapter.

Organizational theories are powerfully heuristic in the case of the IC, but they are not comprehensive. Numerous explanations exist for the IC's perceived failure to collaborate effectively. A distinct and complementary set of theories explaining why the IC doesn't share information is based on the nature of the information with which the IC works.

The Nature of Intelligence Information

The commodity of the intelligence community is information. Mark Lowenthal defines information simply, and fittingly, as "anything that can be known, regardless of how it may be discovered."[29] Typically, intelligence information is obtained by the IC via sources and methods that the IC wishes to protect. In this case, the agency that attains the information is expected to protect it by classifying it appropriately. According to Director of Central Intelligence Directive 1/7, Security Controls on the Dissemination of Intelligence Information, "the originator of intelligence is responsible for determining the appropriate level of protection prescribed by classification and dissemination policy. Originators shall take a risk management approach when preparing information for dissemination."[30] This means that the agency that collects the information determines who will be given access to the information. In essence then the collecting agency becomes the owner of the information. It is the ownership and ability to control access to information that is at the core of IC concepts of knowledge as power, and is the foundation for much of the documented success of the American IC in supporting

29. Mark M. Lowenthall, *Intelligence: From Secrets to Policy*, Second Edition (Washington D.C.: CQ Press, 2003), 1-2.

30. Director of Central Intelligence, DCID 1/7, n.p., online, Internet 25 January 2005, available from https://ia.gordoin.army.mil/ iaso/DCID/17/dcid1-7.html.

military and policy goals. It is also the foundation of the need-to-know system of protecting information.

The need-to-know system of protecting information relies on the assumption that the costs of not sharing information outweigh the perceived risk of inadvertent disclosure. This assumption finds its roots in the earliest days of the intelligence community, when the amount of information available was scarce, and thus needed to be protected. As the intelligence community grew so did its ability to collect information. More information does not necessarily translate into better decision-making, however. With the ability to collect (and capacity to store) increasingly sizeable amounts of information came the requirement to expand control and restriction of access to that information—simply because the classification policy of the IC in an era of scarcity did not change over time. The IC's orientation towards secrecy is exemplified in a 1950 National Security Council directive, which advised "any publicity, factual or fictional, concerning intelligence is potentially detrimental to the effectiveness of an intelligence activity and to the national security."[31] Protecting information to this level creates the perception that the information an agency or individual holds has great value. It is this *perception* of the value of information that is under examination here.

Calculating the true value of information resources is done much the same as for any commodity. Two components are essential—exchange value and operational value.[32] The exchange value is determined in the information free market simply by how much someone is willing to pay for the resource. Since the government is the only legal consumer of the resource, it has a *monopsony* (that is, a buyer's monopoly) in the market and therefore can artificially determine the amount it is willing to pay.[33] This leaves the operational value of information, "determined by the benefits that can be derived from

---

31. NSC Intelligence Directive No. 12, "Avoidance of Publicity Concerning the Intelligence Agencies of the U.S. Government," 6 January, 1950. Reprinted in "Emergence of the Intelligence Establishment," *Foreign Relations of the United States*, 1945-1950 (U.S. GPO, 1996), 1118-1119.

32. Dorothy E. Denning, *Information Warfare and Security* (New York: ACM Press, 1999), 23.

33. This artificial valuing of information is in fact what leads some individuals to sell classified information. When the artificial value is low relative to the individual (access is easy or convenient) and a buyer is willing to pay more than the artificial price (combined with risk assessment) of the resource (determined from the individual producer's perspective), then the resource is stolen and sold illegally. On the dynamics of monopsonies and individual action, see Alan Manning, *Monopsony in Motion: Imperfect Competition in Labor Markets* (New Haven, CT: Yale University Press, 2005).

the resource," as the most accurate determinant of intelligence information.[34] Operational value is not a precise measurement, however. It varies between individuals and organizations, and in the context of time and place. Indeed, one of the most important operational determinants of intelligence value is timeliness; another is completeness. For the purposes of this investigation, these contextual values are subsumed by the overarching operational value that is simply the *availability* of the resource to the individual or agency. It is availability that provides the individual or agency the opportunity to use the information in whatever way appropriate. Unavailable information, in this schema, is valueless—and may even have negative value.[35] In this manner, information is viewed as a commodity, which, according to Karl Marx, is "a thing that by its properties satisfies human wants of some sort or another."[36]

Since the operational value of intelligence derives in part from the exclusivity of information, namely the ability to keep information resources out of the hands of opponents and adversaries, the perception is that by "being the only player or one of a few players with access to [limited] information is worth more than having access to information that is widely known."[37] Being able to control scarce information then translates into power within the intelligence community because information is often used in competitive situations in which one nation, agency, or individual is trying to obtain an advantage over another.[38] Thus by protecting and hoarding information, both the agency and the individual promote the (at least implicit) goals and objectives of the agency, to include any reduction of relative influence within the organization. Some examples protection of bureaucratic or agency objectives include seeking to avoid decreases in budget, both absolute and relative to other agencies; decreases in manpower,

---

34. Denning, Information Warfare, 24.

35. Imagine a situation in which a decision-maker knows information exists that could provide certainty in the choice to be made, but is not allowed (or otherwise unable) to obtain it. That decision-maker will likely delay decisions, in hope the information my become available, or will overly second-guess the decision, reducing the longer-term capacity to make future decisions.

36. Karl Marx, "The Two Factors of a Commodity: Use-Value and Value," in Charles Lemert (ed.), *Social Theory: The Multicultural and Classic Readings*, Second Edition (Boulder, CO: Westview Press, 1999), 51.

37. Denning, Information Warfare, 23.

38. Joseph S. Nye Jr., Power in the Global Information Age: From Realism to Globalization (New York, NY: Routledge, 2004), 88.

especially in key specialties; and reducing or deflecting encroachment by other agencies on that agency's traditional or assigned roles and missions.[39]

The operational value of information, in use and in potential, assists in the promulgation of the now widely held paradigm that information is power. That information is a component of state or national power, however, is a relatively recent notion. Hans Morganthau, dean of American international relations theorists, defined the elements of national power as geography, natural resources, industrial capacity, military preparedness, population, national character, national morale, and the quality of diplomacy and government.[40] Nowhere in his post-WW II description is information seen as an instrument of power. Rather, information manipulation was a vital, if unseemly, tool of diplomacy and the Department of State, and that is where it was to be kept safely in the hands of secure professionals.

The paradigm cracked in 1962, when Adlai Stevenson confronted Soviet Representative Zorin on the floor of the UN Security Council with images of the San Cristobal MRBM site, taken on a highly classified U-2 reconnaissance mission during the Cuban Missile Crisis.[41] Until this remarkable world-changing event, Cold War intelligence had not been released in so public a fashion (or to so many, with the advent of television). Perhaps for the first time, the use of information as an element of national power was based not on its exclusivity (in an earlier day, the information might have been revealed to a few Soviet diplomats behind closed doors), but on its broad dissemination.[42] This was not the first time that intelligence information had been placed into the public forum, but it is undoubtedly one of the most dramatic.[43] And so it is with this momentous incident that the transition from the concept of secret or hoarded

---

39. Allison and Zelikow, *Essence of Decision*, 168-170.

40. Hans J. Morganthau, *Politics Among Nations: The Struggle for Power and Peace* (New York: Alfred A. Knopf, 1967), xviii.

41. Michael R. Beschloss, *The Crisis Years: Kennedy and Khrushchev, 1960-1963* (New York, NY: Edward Burlingame Books, 1991), 505-506; also Dino A. Brugioni, *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis* (New York: Random House, 1991), 425-429.

42. In this case, the image was collected and provided by an intelligence agency of the United States, which, prior to its public release by the President, had the ability to control access to the image.

43. An example of intelligence used in the public forum was the publishing of the "Zimmerman Telegram" by the American Press prior to US entry into World War I—though this action, as with many other similar examples, was more associated with the power of the press than the power of the state. Barbara Wertheim Tuchman, *The Zimmerman Telegram* (New York: Viking Press, 1958), 185-187.

information comprising a portion of state power to one where open or shared information is perceived as vital and legitimating component of state power.

According to Dan Kuehl, "The world in which we live and work has become an information fishbowl."[44] But, more information is not always a good thing. Without the capacity to interpret, understand, and use it, it can be more of a hindrance than a help. According to Joseph Nye, there are three dimensions, or aspects, that contribute to a comprehensive understanding of information: 1) the flows of data such as news and statistics, 2) information used for advantage in competitive situations, and 3) strategic information or knowledge of your enemies' game plans.[45] While any theory if information power must incorporate an understanding of all three, it is the third dimension with which the intelligence community is most concerned.

Knowledge of the enemy is one of the primary reasons the US intelligence community exists. The desire to obtain knowledge of the enemy and its plans has led to large investments in collection systems to provide the raw information the intelligence community needs to obtain this knowledge. Yet, as the collection capabilities of the IC grows, so does the "paradox of plenty."[46] The more information that is collected, the more overwhelmed the IC becomes with the sheer volume of information. In such a case, *attention*, rather than information, becomes the scarce resource, and *those who can distinguish the valuable signals from all the noise* become powerful. "The most important concept to remember about information is that it is not a weapon per se ;it is a process."[47] Power does not flow to those who can produce and withhold information; power goes to those who can transform information by sorting out what is correct and important, and then ensuring those who need it have access to it. It is this requirement to process and transform information that is driving the IC to a new paradigm in which *sharing* information is power—not hoarding it.

Hence a new paradigm for the use and control of information in the intelligence community is rapidly forming out of the old need-to-know system into a need-to-share

---

44. Dan Kuehl, "Foreword," in Leigh Armistead (ed.), *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington D.C.: Brassey's, Inc., 2004), xviii.

45. Nye, Power in the Global Information Age, 88-89.

46. Hebert A. Simon, "Information 101: It's Not What you Know, It's How You Know It," *The Journal for Quality and Participation* (July/August 1998), 30-33.

47. Leigh Armistead, "Introduction" in Armistead (ed.), *Information Operations*, 1.

concept. The need-to-know system "assumed that it was possible to determine *a priori* who needed to know particular information."[48] However, in light of the challenges facing the IC as it deals with a diverse and ever-expanding threat from rogue states and international terror, it is far more critical that information get to the very many who need it in as timely a fashion as technology allows. This tends to confound the rational-economic models of theorists, who have a hard time explaining why self-interested individuals would freely share a scarce resource. In part, the solution comes from the increasing abundance of information, and from the notion that information is a "non-rival" good, that is, one person's use of it does not interfere with another's use of the same information.[49] Viewing intelligence information in this way, coupled with cooperation on sharing the information within the IC, which when repeated builds trust and reciprocity, could act to benefit the IC as a whole.

Unfortunately, if one accepts the notion that the very foundations of information as power is undergoing a profound change, current decisions about sharing intelligence in the government are still made largely in the context of a system of classification that was developed during the Cold War.[50] This classification system enables and then fosters some of the group dynamic and collective action problems from which the IC has long suffered.

Group Dynamics as the Catalyst for Not Sharing

Mancur Olson, in his path breaking book *The Logic of Collective Action*, defines a group as "a number of individuals with a common interest."[51] It has traditionally been assumed that the members of a group will work to attain the goals or common interests of the group. Indeed, efficient acquisition of common goals and interests is the precise reason for establishing the group. Therefore, "groups of individuals with common interests are expected to act on behalf of their common interests much as single

48. Markle Foundation, *Task Force on National Security in the Information Age*, n.p. on-line, Internet, 26 June 2005, available from, http://www.markletaskforce.org/about.html.

49. "The Economics of Sharing," *Economist*, 5 February 2005, 72.

50. House, House Committee on Government Reform, Subcommittee on National Security, "Emerging Threats, and International Relations – Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing," 24 August 2004, Testimony of Bill Crowell, Markle Taskforce on National Security in the Information Age, on line, Internet 25 June 2005, available from http://www.fas.org/sgp/ congress/ 2004/082404crowell.html.

51. Olson, *Logic*, 8.

individuals are expected to act on behalf of their personal interests."[52] Reality shows us that this is rarely the case. Members of a group, barring some form of coercion or inducement, are more likely to focus on maximizing personal welfare prior to advancing any of the common or group objectives—if addressing them at all. This drive to maximize personal welfare then leads to politicization of the group environment.

"Most people working in an organization readily admit in private that they are surrounded by forms of 'wheeling and dealing' through which different people attempt to advance specific interests."[53] The drive that individuals exhibit to advance specific interests is an integral component in the historical failure of the IC to put forth an optimal collective effort. Conflict arises whenever interests collide. Interests are predispositions towards goals, values, desires, and expectations that lead an individual to act in a certain way.[54] The conflict may be personal, interpersonal, or between rival groups, but it is this clash of individual interests that creates the political atmosphere of the community.

Olson takes pains to differentiate groups based on size. Small groups are defined as those in which every member has direct relationships with every other member, and can evaluate the contribution (or lack thereof) of each. Intermediate groups are those in which any member could develop at least a passing relationship with any other and that special or large contributions to the collective good could make a difference large enough to be noticed. Large groups are such that it is impossible to have even a passing awareness of and relationship with every other member, and the contribution of any single member makes little or no discernible impact on the total provision of the group good. In Olson's words, the three factors that keep large groups from furthering their own interests are:

> First, the larger the group, the smaller the fraction of the total benefit any person acting in the group receives. Second, since the larger the group, the smaller the share of the total benefit, the less the likelihood that nay small subset of the group, much less any single individual, will gain enough from getting the collective good to bear the burden of providing even a small amount of it. Third, the larger the number of members in the group the greater the organization costs, and thus the higher the

52. Ibid., 1.

53. Gareth Morgan, *Images of Organization*, Second Edition (Thousand Oaks, CA: Sage Publications, 1997), 154.

54. Ibid., 161

> hurdle that must be jumped before any of the collective good at all can be obtained.[55]

With these factors as the basis of his comprehensive theory, Olson points out that small groups will quite routinely achieve large or even optimal amounts of the common good, as one or more members may be willing to take on the burden of providing the collective good for everyone else. This is quite common in familieas, for instance, or when one diner picks up the check for the whole table. Intermediate-sized groups *may* achieve significant amounts of the group good, particularly if a small subset of the members (a committee, perhaps) can be persuaded to take on an unfair share of the group burden, and while the total group good is likely to be adequate, it is very unlikely to be optimal (satisfying for all with little or no waste). Large groups will not achieve even scant amounts of the group good without incentives and/or punishment to coerce the individual members to act in the best interests of the whole.

The IC has characteristics of, and can be viewed as, both an intermediate group-of-groups, or a very large group of individuals. The IC consists of fifteen different agencies, all of which try to work together in order to provide intelligence information to the leaders of the United States in support of national security.[56] It also conducts much of its business through National Centers, which are organizations or groups created to address specific non-traditional threats.[57] The centers are nothing more than additional groups within the IC that suffer from the same problems as the IC as a whole, and that add to the membership size of the group-pf-groups that comprise the IC.

Personnel for the Centers come from the agencies that make up the IC. The argument in support of the Centers is that by physically locating individuals engaged in

---

55. Olson, *Logic*, 48

56. National security is a classic example of what Olson defines as a group or collective good. It meets the dual criteria that if it is available to one member of the group, then it is available to all, and that the amount of consumption by any one member of the group does not diminish the amount any other member may consume. National security that comes from a policy of nuclear deterrence, for example, is provided to every member of the state, regardless of the amount of satisfaction or safety the individual may take from it.

57. US Intelligence Community Website, online, internet 15 January 2005, available at http://www.intelligence.gov/2-community_centers.shtml. Some of the examples of National Intelligence Centers include: the Weapons Intelligence, Nonproliferation and Arms Control (WINPAC), the Counterterrorist Center (CTC), the Crime and Narcotics Center, the Information Analysis and Infrastructure Protection, the National Drug Intelligence Center, The El Paso Intelligence Center, the Directorate for MASINT and Technical Collection, the National Counterterrorism Center, the Terrorist Screening Center, and the National Virtual Translation Center.

common problems at the same location, regardless of their parent organizations, the Centers will become the catalyst for the sharing of information across the IC. Viewing the IC as an intermediate size group, the concept has merit. However, as the individuals working in the Centers continue under the rules of (including pay and promotion) their parent organizations—and can expect to return to that organization at the end of their tour in the center—simply combining them does not provide the necessary incentives to promote large group goals. From the large group perspective, individuals working in the various centers have personal incentives to first work to meet their own goals and objectives, then focus on the goals and objectives of their parent organization, before finally allowing themselves, if time and resources permit, to work on the goals and objectives of the Center itself. "The problem with the Centers is that they are separated from the budgeting process which creates a dilemma for the traditional agencies. For example if the Director of State/INR makes all his analysts available to work in the Centers and then doesn't produce analysis for the State Department itself, the budgeting process would penalize his organization due to the lack of production."[58]

Conclusion

Each of the theories expanded upon above provide a viable explanation as to why the IC is not willing to share intelligence information. Each accepts the premise that organizations exist in order to achieve the needs of the organization in the most efficient and effective means possible. However, each finds inherent structural limitations that prevent the organization from achieving goal optimization. Allison and Zelikow's Model II behavior reveals that organizations, when faced with conflicting goals, will satisfy one while deferring the other. Accordingly, when an IC agency is faced with the conflicting goal of doing what is best for the IC versus doing what is best for the individual agency, organizational theory shows that we can expect the agency to focus on itself first, and the IC as a whole second.

Theories on the nature of intelligence information reveal that information can be, and often is, viewed as a commodity within the IC. This commodity has value, and is therefore protected by the agency that owns the information. The traditional manner in

58. Jon Wiant, Ph.D., Faculty member at the Joint Military Intelligence College, interviewed by author, 24 June 2005.

which the IC protected its information was through the need-to-know system of limited access. The ability to control access to information then translates into the perception of special kind of information power, both for the individual and for the agency that controls access to the information. However, the nature of information power appears to be changing as information itself is growing abundant.[59] This changing paradigm is challenging the IC to develop new ways to view information and information power. While the ability to limit access to information is still the dominant view, the ability to influence public debate through broad release of classified information, as was done during the Cuban Missile Crisis, is increasingly perceived as legitimate information power. Thus power, as perceived by the IC, is becoming the ability to control *and* influence through the use of intelligence information.

Finally, the way groups and individuals act and interact provides additional insight for a broader theoretical framework explaining why IC agencies and individual's don't share information. It was further shown, compatible with the organizational theoretical perspective first discussed, that when faced with a dilemma of competing priorities, individual IC analysts will tend to focus first on priorities that advance their personal goals before those of their parent organization, and *last* on the priorities of the intelligence center to which they might be assigned.

Although all three theories are compelling in their own right, the interaction of the three provides a compelling rationale for why the IC should be *expected* to operate suboptimally—if not dysfunctionally—in its work. The next step in this theoretical argument is to test these theories individually and in the aggregate against evidentiary data. The following chapters will look at three specific timeframes in the history of the IC. The first follows the creation of the IC and its evolution through the Cold War. The second examines several post-Cold War events prior the 11 September, 2001 terrorist attacks. The third discusses the events that led to this attack, the investigation that resulted, and the recommendations that have been implemented as a result of this investigation.

---

59. More *is* different, according to the new proponents of complexity theory. See Edward O. Wilson, *Concilience: The Unity of Knowledge* (New York: Vintage, 1998), 96-9; and M. Mitchell Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos* (New York, NY: Touchstone, 1992), 9-13.

Chapter 3

The Cold War

Creation, Evolution, and Reformation of the IC

Although the US intelligence community can trace its lineage to before the American Revolution, the drive to coordinate the disparate agencies that make up what would eventually be known as the IC is rooted in the American experience from World War II through the end of the Cold War. For the intelligence community, this part of its history is bounded by two intelligence failures – the failure to predict the Japanese attack on Pearl Harbor and the failure to predict the collapse of the Soviet Union.

World War II

Without question, the near total war experience of World War II was the the catalyst and organizational incubator for the establishment of what we call today the intelligence community. It was obvious that the United States would no longer have the luxury of isolationism, and a return to the minimal pre-war intelligence structure it had held was not an option. With the rise of a new kind of enemy in the US-Soviet Cold War, the National Security Act of 1947 created the intelligence bureaucracy that in modified form remains in effect today. And yet, even though the framers of this organization were cognizant of the many problems that bedeviled the performance of the intelligence community in the recent global war, the structure they instituted would work to ensure these problems continued.

US entry into World War II is marked by what was once considered the greatest intelligence failure in history – the failure to anticipate the Japanese attack on Pearl Harbor. However, as Roberta Wohlstetter points out in *Pearl Harbor: Warning and Decision*, this was not so much a failure of intelligence, but a failure of analysis. In her work, Wohlstetter shows that while all of the information needed to anticipate Japan's attack on Pearl Harbor was available, "no single person or agency ever had at any moment all of the signals existing in this vast information network. The signals lay

scattered in a number of different agencies; some were decoded, some were not; some traveled through rapid channels of communication, some were blocked by technical or procedural delays; some never reached a center of decision."[1]

In the investigation of the performance of both Army and Naval intelligence prior to the attack, all three of the bases for not sharing information in the previous chapter can be readily found. Organizationally, the two services essentially agreed to disagree. An overarching desire to protect the sensitive information they were collecting from any who might compromise it, including the other services, further led to a failure of analysis. In doing so, each group worked to ensure the importance of the group or agency first before turning to the true objective at hand, which was to monitor the Japanese military movements and political intent.

For much of the 1930s, the Army's Signal Intelligence Service and the Navy's Code and Signal Section were not on speaking terms, as the two sought to independently crack "the same diplomatic codes and ciphers 'to gain credit for itself as the agency by which the information obtained was made available to the government.'"[2] This inter-service competition carried forward to the task of decrypting Japanese diplomatic traffic once the code was broken. In order to prevent either service from gaining an analysis advantage over the other, "it was agreed…that the Army and Navy would exchange all diplomatic traffic from their intercept facilities… But in order to avoid as much duplication of effort as possible it was agreed that the Army would receive all traffic of days with an even date and the Navy all traffic of days with an odd date."[3] This arbitrary division of effort cannot be justified in any rational cost-utility analysis, but is at least comprehensible in the theoretical perspectives of organizational, informational, and collective action theories. In fact, the competition between the two agencies and services went as far as determining who would deliver the decrypted information to the President. Once again, in a compromise, the two services decided that MAGIC information would

---

1. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), 385.

2. Christopher Andrew, For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush (New York, NY: Harper-Perennial, 1995), 104.

3. Christopher Andrew, "Codebreakers and Foreign Offices," in Christopher Andrew and David Dilks (eds.), *The Missing Dimensions: Governments and Intelligence Communities in the Twentieth Century*, (London: Macmillan, 1984), 52-53.

be delivered by Roosevelt's naval-aide in even numbered months and by his military-aide in odd numbered months.[4]

Investigations into pre-attack intelligence also showed much of it had been handled in a casual manner, and that the lack of coordination, primarily between the Army and Navy, resulted in key decision makers not having the information they needed. Another problem that prohibited effective analysis of the collected information was the desire to protect MAGIC information. Those that had access only had it briefly, and this limited their ability to assess it in context with other intelligence.[5] "They were also generally wrong in their assumptions about who else saw it," and this impacted their decisions to provide warning to either the theater or to the policymaker, as the analysts assumed that both were already aware of the information.[6] In these instances, the desire to protect the information prevented analysts from collaborating on and discussing it with those who needed it. The operational need for decision makers in Washington and at Pearl Harbor to know about information contained in the intercepts was unable to overcome the perceived need to protect the source of the information.

The group dynamics related to President Roosevelt's attempts to force collaboration—or at least information sharing during the War—is also very revealing. Roosevelt began the process of attempting to remedy the problem as early as April 1941.[7] In a Cabinet meeting, the president discussed the problem of lack of coordination between intelligence agencies and noted that the way the British dealt with the problem was to have a single individual responsible for settling disputes. Out of fear that Roosevelt was going to create the same kind of office in the US intelligence structure, the army assistant chief of staff for intelligence wrote to General Marshall that:

> In great confidence O.N.I. tells me that there is considerable reason to believe that there is a movement afoot…to establish a super agency controlling all intelligence. This would mean that such an agency…would collect, collate and possibly evaluate all military intelligence that we now gather from foreign

4. David Khan, "Roosevelt, MAGIC, and ULTRA," *Cryptologia*, 14 (1992), 292. MAGIC was the codename used to identify the intelligence information derived from the decryption of Japanese communications.

5. Wohlstetter, *Pearl Harbor*, 186.

6. Ibid.

7. Henry Stimson, "Notes After Cabinet Meeting, April 4, 1941," as found in Troy F. Thomas, "The Coordinator of Information and British Intelligence," *Studies in Intelligence*, 18, no. 1-s (Spring 1974), 90.

> countries. From the point of view of the War Department, such a move would appear to be very disadvantageous, if not calamitous.[8]

President Roosevelt did in fact create a Coordinator of Information (COI), and placed it under William Donovan, then an emissary for the President.[9] Donovan agreed to take the job under the condition that "all departments of the government would be instructed to give him what he wanted."[10] This strong plan for centralization quickly ran into opposition from the Departments of War, Navy, and State, as well as the Justice Department's FBI, all of whom conducted intelligence activities of their own. The one thing they all could agree on was "that they did not want a strong central agency controlling their collection programs."[11] Donovan was never able to overcome the turf battles that waged throughout the US intelligence community, and Roosevelt disbanded the COI in favor of a new Office of Strategic Services (OSS) that would report to the Joint Chiefs of Staff instead of the President. Even this did not end the internal bickering. Within a year of its creation the OSS was accused of seeking to reduce G-2 and ONI "to the status of reporting agencies and research bureaus."[12] As the war neared an end, it was going to be necessary to decide what to do with the intelligence organizations and capabilities that the nation now had. This was one of the problems left to President Truman.

National Security Act of 1947

Harry Truman did not learn of all of the US government's intelligence activities until after he became President in April 1945. Even so, it would be up to Truman to decide what to do with these intelligence capabilities once the war was over. Truman decided to disband the OSS in September 1945 partly because of reports that the OSS had conducted "overlapping and unauthorized activities with resulting embarrassment to the State Department and interference with other secret intelligence agencies of this

---

8. Miles to Marshall, 8 April 1941, as found in Thomas, "The Coordinator of Information," 88.
9. Thomas F. Troy, *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency* (Frederick, MD: Aletheia Books, 1981), 29-34.
10. Ibid., 62-70.
11. Ray Cline, *The CIA Under Reagan, Bush, and Casey* (Washington: Acropolis Books, 1981), 112.
12. Bradley F. Smith, *The Shadow Warriors* (London: Andre' Deutsch, 1983), ch. 3.

government."[13] By executive order the Research & Analysis section of the OSS was given to the State Department while the espionage and counterespionage portions went to the Army as a new Strategic Services Unit.[14]

Truman still faced the problem of coordinating the foreign intelligence efforts of the government, and he turned to Secretary of State Byrnes for help. Apparently frustrated by the large number of conflicting reports he received, Truman asked Secretary of State Byrnes to "take the lead in developing a comprehensive and coordinated foreign intelligence program for all Federal agencies concerned with that type of activity. This should be done through the creation of an interdepartmental group, heading up under the State Department, which would formulate plans for my approval."[15] This directive created infighting among the heads of the army, navy, FBI, and State Department, as all tried to protect their departmental prerogatives from outside interference.[16]

The outcome of these turf battles was a presidential directive which established a National Intelligence Authority (NIA) composed of the secretaries of state, war, the navy, a presidential representative, and a Director of Central Intelligence (DCI). The NIA was to "plan, develop, and coordinate…all Federal intelligence activities," while the DCI was to attend NIA meetings as a non-voting member and direct the work of a new Central Intelligence Group (CIG), a small interdepartmental group responsible for coordinating, planning, evaluating, and disseminating intelligence. Ultimately, however, the DCI and thus the CIG were controlled by the NIA.[17]

Efforts by the DCI to consolidate intelligence reports for the President via the CIG as requested soon ran afoul of the State Department. Secretary of State Byrnes refused to turn over State cables to the CIG "on the grounds that it was his responsibility alone to inform the president of the cables' contents."[18] The CIG director was forced to

---

13. Colonel Richard Park, Jr., "Memorandum for the President," Rose Conway File, n.d., box 15, File OSS/Donovan, HSTL. As cited in Andrew, *For the President's Eyes Only*, 156.

14. EO 9621**,** "Termination of the Office of Strategic Services and Disposition of its Functions," 20 September 1945, as found in Troy, *Donovan and the CIA*, 294-302.

15. Truman to Byrnes, 20 September 1945, as found in Troy, *Donovan and the CIA*, appendix T.

16. Andrew, For the President's Eyes Only, 164.

17. Daniel Yergin, Shattered Peace: The Origins of the Cold War and the National Security State (Boston, MA: Houghton Mifflin, 1977), 216-217.

18. Andrew, For the President's Eyes Only, 165

turn to Truman for mediation, and Truman sided with the CIG, another example of the interdepartmental fighting that surrounded the creation of the CIG.

The watershed moment for the US intelligence community was the passage of The National Security Act of 1947 unified the military under a Department of Defense, created the National Security Council, and established the Central Intelligence Agency (CIA), "for the purpose of coordinating the intelligence activities of the several Government departments and agencies in the interest of national security."[19] The portion of the law that created the CIA is remarkably vague. Under the Act the CIA was responsible:

> (1) to advise the National Security Council in matters concerning such intelligence activities of the Government departments and agencies as relate to national security;
> (2) to make recommendations to the National Security Council for the coordination of such intelligence activities of the departments and agencies of the Government as relate to the national security;
> (3) to correlate and evaluate intelligence relating to the national security, and provide for the appropriate dissemination of such intelligence within the Governments using where appropriate existing agencies and facilities: *Provided*, That the Agency shall have no police, subpoena, law-enforcement powers, or internal-security functions: *Provided further*, That the departments and other agencies of the Government shall continue to collect, evaluate, correlated, and disseminate departmental intelligence: *And provided further*, That the Director of Central Intelligence shall be responsible for protecting intelligences sources and methods from unauthorized disclosure;
> (4) to perform, for the benefit of the existing intelligence agencies such additional services of common concern as the National Security Council determines can be more efficiently accomplished centrally;
> (5) to perform such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct. [20]

The wording of the National Security Act that relates to the CIA reflects the self-interests of each affected agency. For example, in spite of the CIA's ability to coordinate intelligence activities, these activities still had to be approved by the NSC. Since both the Secretary of State and the new Secretary of Defense were members of the NSC, they

19. US Code Congressional Service, *Laws of the 80th Congress*, 1st sess. (St Paul, MN: West Publishing Co., 1947), 502.

20. Ibid.

would be able to significantly influence if not veto and any recommendations the DCI might make. Therefore, all activities of the CIA required the cooperation of both State and Defense Department leadership. It is also clear that the CIA was not going to supplant any other department's intelligence collection, evaluation, correlation, or dissemination abilities, meaning that each department would continue to provide for its own intelligence support without having to rely on or collaborate with the new CIA.

The Cold War

During the Cold War, as America's need to peer through the iron curtain generated an intensified national intelligence effort, examples of non-collaboration within this community stepped up. Investigations into why the administration had no warning about the North Korean attack into South Korea revealed that "defects in handling SIGINT" before the war "were strikingly similar to those before Pearl Harbor."[21] Apparently, while Truman had been trying to improve US SIGINT capabilities when he created the Army Security Agency (ASA), it had had the opposite effect.

After V-J Day, the Navy tried to reclaim its share of pre-Pearl Harbor diplomatic traffic, but the ASA refused to give up its monopoly. Meanwhile, the newly created Air Force was given a SIGINT capability of its own, further complicating the situation. The first attempt to resolve this confusion failed.[22] However, a second attempt resulted in the creation of the Armed Forces Security Agency (AFSA). But the investigation (known as the Brownell Committee) into the failure of the AFSA to provide adequate warning prior to North Korea's invasion found that the problem was primarily disarray:

> In theory the Joint Chiefs of Staff exercise direction over the AFSA. In practice this direction is taken over almost entirely by their agency AFSAC, which is an interservice committee acting under the rule of unanimity. Its members devote much of their time in frustrating detail to safeguarding individual Service autonomies. The Director of AFSA is obligated to spend

21. Andrew, For the President's Eyes Only, 185.

22. In August 1948, Secretary of Defense James V. Forrstal created a board under the chairmanship of Rear Admiral Everett Stone, then Director of Naval Communications, to study the COMINT situation within the defense establishment and recommend a solution. The Stone Board went round and round for several months but wound up submitting a divided report – the Navy and the Air Force both opposed consolidation, the Army advocating it with the exception of interception and decentralized field processing stations. Unhappy with the results, Forrestal simply locked the report in a safe and hoped the problem would go away. See James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (New York, NY: Penguin Books, 1982), 70-71.

> much of his energy on cajolery, negotiation, and compromise in an atmosphere of interservice competition. He has no degree of control, except by making use of such techniques, over the three COMINT units operated by the Services. In fact he is under the control of the three Service unites, through their respective representation on AFSAC. His only appeal is to the same three Services sitting as the Joint Chiefs of Staff.[23]

This is an illuminating example of an organization protecting its interests by not sharing information, as well as an intriguing example of how intelligence-specific groups act and interact. The Brownell Committee condemned the "duplication of effort" and "wasteful and inefficient practices" of the rival agencies.[24]

In an attempt to address the SIGINT community's infighting, Truman abolished the AFSA and created a new organization called the National Security Agency (NSA) tasked to "produce SIGINT 'in accordance with the objectives, requirements and priorities established by the Director of Central Intelligence Board.'"[25] As indicated by the name change, NSA's focus extended beyond just the military. In an awkward organizational structure, NSA was considered "within but not part of DOD."[26] Additionally, the DOD directive that created NSA gave the Director of NSA the mission of prescribing "within his field of authorized operations requisite security regulations covering operating practices, including the *transmission, handling, and distribution of SIGINT material* within and among the elements under his control."[27] Here is an example of the organization being given the ability to control access to the information it "owns." In effect, the ability of NSA to control access increased the operational value of the information it had.

Other organizational changes that took place during the Cold War were intended to either develop a new technology or to resolve inter-agency or inter-service rivalries. In 1961, the National Reconnaissance Office (NRO) was created to oversee the development and launch of reconnaissance spacecraft, as well as to disseminate the data

---

23. Ibid., 77-78.

24. George Brownell, *The Origin and Development of the National Security Agency* (Laguna Hills, CA: Aegean Park Press, 1981), 37-39.

25. NSCID No. 6, "Signals Intelligence," 17 February 1972; Department of Justice, *Report on CIA-Related Electronic Surveillance Activities* (Washington D.C.: Department of Justice, 1976), 77-78.

26. National Security Agency/Central Security Service, *NSA/CSS Manual 22-1* (Ft. Meade.: NSA 1986), 1.

27. Emphasis added. Department of Defense Directive S-5100.20, "The National Security Agency and the Central Security Service," 23 December 1971.

collected. With dissemination of the data came the responsibility to "establish security procedures to be followed for all matters of the National Reconnaissance Program and... to protect all elements of the National Reconnaissance Office."[28] These security procedures included determining the criteria for granting access to information about these programs as well as determining the physical security requirements of the documents relating to those programs. Like NSA, the NRO was given the ability to preclude other IC agencies or analysts from having access to information it collected, and again this allowed the NRO to increase the perceived operational value of the information it controlled. This created another barrier to effective collaboration—because of the analyst's inability to readily discuss NRO-derived information.

Another reorganization of the IC during the Cold War created of the Defense Intelligence Agency. "Faced with the disparate estimates of Soviet Missile strength from each of the armed services which translated into what have been called self-serving budget requests for weapons of defense, the United States Intelligence Board created a Joint Study Group in 1959 to study the intelligence producing agencies."[29] This study group found that there was considerable duplication and overlap between the service intelligence agencies, and that this overlap made the "overall direction and management of DOD's intelligence effort…a difficult if not impossible task. Indeed, the fragmentation of effort creates 'barriers' to the free and complete interchange of intelligence information among the several components of the Department of Defense."[30] The compromise organization resulting from this study was a DIA that reported to the Secretary of Defense *through* the JCS. Nonetheless, each service was allowed to keep portions of its intelligence functions, with the Director of DIA reviewing and coordinating the service intelligence function's activities.[31] Thus the creation of DIA did not necessarily end inter-service fighting or increase the level of collaboration on intelligence estimates: it merely added another bureaucratic layer to the overall fight.

---

28. Department of Defense Directive TS 5105.23, "(S) National Reconnaissance Office," 27 March 1964, 4. Previously declassified.

29. US Congress, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Final Report, Book VI: Supplementary Reports On Intelligence Activities* (Washington, D.C.: US Government Printing Office, 1976), 266.

30. Jeffrey T. Richelson, *The US Intelligence Community*, Fourth Edition (Boulder, CO: Westview Press, 1999), 55.

31. Ibid., 57.

These three organizational developments reveal a trend within the IC that carried through the Cold War—to protect or restrict access to the information an agency held, while at the same time fostering the prestige of the agency itself, thus fulfilling the agency or organization's goals.

The Cold War also saw numerous attempts to reform the IC in order to make it more efficient. The first of these came just one year after the IC was created. In 1948 President Truman commissioned the first study of the IC. The resulting Dulles-Jackson-Correa report found that the CIA was not drawing on the work of the other agencies in its preparation of estimates; rather it was producing estimates based on its own analysis and offering these in competition with similar products from other agencies.[32] Despite its findings, the Dulles-Jackson-Correa report did not make any recommendations for correcting the problem other than relying on the goodwill of the agencies involved.

Also during 1948, Congress established "The Commission on Organization of the Executive Branch of Government," which became known as the First Hoover Commission after is Chair, former President Herbert Hoover. The Commission established a sub-group to examine national security organizations, including the CIA. The report of this group, headed by Ferdinand Eberstadt (which became known as the "Eberstadt Report"), found that "the relationships of this agency [CIA] to some of the intelligence agencies of the Government–notably to G-2 of the Army, the Fedreal Bureau of Investigation, The Atomic Energy Commission, and the State Department have been and still are unsatisfactory."[33] In this report, the military and State Department were faulted for not sharing pertinent information with the CIA. The Commission recommended that "vigorous efforts be made to improve the internal structure of the Central Intelligence Agency and the quality of its product…and that positive efforts be made to foster relations of mutual confidence between the Central Intelligence Agency and the several departments and agencies that it serves."[34]

---

32. Allen W. Dulles, Mathias F. Correa, and William H. Jackson, *The Central Intelligence Organization and National Organization for Intelligence*, n.p., on-line, Internet, 30 June 2005, available at http://www.state.gov/www/ about_state/history/intel/350_359.html.

33. Ferdinand Eberstadt, *National Security Organization*, Appendix G (Washington D.C., US Government Printing Office, 1949), 76. Hereafter cited as the Eberstadt Report.

34. Ibid., 16.

A second Hoover Commission was convened by Congress in 1954. This time the sub-group tasked with examining the intelligence agencies, headed by General Mike Clark, made only one recommendation, that the "the President appoint a committee of experienced citizens to examine and report to him periodically on the government's foreign intelligence activities."[35] The task force was also concerned about the amount of intelligence information that was being collected on communist countries, and warned that "the glamour and excitement of some angles of our intelligence effort must not be permitted to overshadow other vital phases of the work or to cause neglect of primary functions."[36] This report is also credited with coining the phrase "intelligence community," although skeptics wondered how "intelligence agencies – jealous of their turf, distrustful of one another, loath to share information, close-chested in their operations," could be called a community.[37]

In December 1970, President Nixon commissioned the Office of Management and Budget to examine the performance and organization of the intelligence community. In March 1971, the report, "A Review of the Intelligence Community," was submitted by OMD Director James R. Schlesinger. Known as the Schlesinger report, the study noted that "the community's heavy emphasis on collection is itself detrimental to correcting product problems. Because each organization sees the maintenance and expansion of its collection capabilities as the principal route to survival and strength with the community, there is a strong presumption in today's intelligence set-up that additional data collection rather than improved analysis, will provide the answer to particular problems."[38] Schlesinger recommended three options for addressing these issues, including: 1) the creation of a Director of National Intelligence, 2) the strengthening of the position of the DCI, and 3) creating a Coordinator of National Intelligence.[39]

---

35. Commission on Organization of the Executive Branch of the U.S. Government (1953-1955), *Intelligence Activities: A Report to the Congress*, 84th Cong, H. Doc. 201, 211. Hereafter cited as the 2nd Hoover Commission.

36. Ibid., 211-212.

37. Thomas Troy, "The Quaintness of the U.S. Intelligence Community: Its Origin, Theory, and Problems," in Loch K. Johnson and James J. Wirtz (eds.), *Strategic Intelligence: Windows Into a Secret World (An Anthology)* (Los Angeles, CA: Roxbury Publishing, 2004), 25-26.

38. James R. Schlesinger, "A Review of the Intelligence Community, March 10, 1971," 11, on line, Internet 25 Jan 2005, available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB144/document%202.pdf. Hereafter cited as the Schlesinger Report.

39. Schlesinger Report, 25-32.

Of the remaining investigations into the performance of the intelligence community during the Cold War, three (the Rockefeller Commission, the Church Committee, and the Pike Committee) focused on the illegal activities of the intelligence community and especially on the CIA in particular.[40] The remaining investigations, the 1975 Commission on the Organization of the Government for the Conduct of Foreign Policy (the Murphy Commission), the 1976 Clifford and Cline Proposals, and the 1985 Turner Proposal, all focused primarily on the Director of Central Intelligence's ability to coordinate the activities of the IC. Each recommended strengthening this role, either through additional authority or with the creation of new stronger position from which to oversee the IC.

Every investigation of the IC that occurred during the Cold War focused on its organizational structure and the DCI's ability to coordinate its efforts. Many of the investigations determined that problems were caused by the infighting and lack of cooperation that occurred between agencies. These reports provide credence to a lack of sharing for reasons projected by organizational behavior theory, and they provide some evidence supporting the lack of sharing as a result of the changing nature of information.

The Cold War came to an abrupt end with the collapse of the Soviet Union. Whether or not the CIA provided enough timely and accurate assessments to lead to projections of the rapid dissolution of the Soviet Union may never be known for certain. Retro-fitted analyses and soul-searching *mea culpa's* aside, perceptions are that the IC in general—and the CIA in particular—did not provide sufficient warning of its impending collapse, and therefore US policymakers were caught unaware. Senator Moynihan, one of the agency's biggest critics, called its performance "shameful."[41] Meanwhile, a *New York Times* editorial opined, "the once proud agency has, at least to public perception, flunked."[42] What is clear is that an agency that had spent the last 40 years focused

---

40. Richard A Best Jr., "Proposals for Intelligence Reorganization, 1949-1996," as found in House, Permanent Select Committee on Intelligence, *IC21: Intelligence Community in the 21st Century*, Appendix C (Washington, D.C.: U.S Government Printing Office, 1996), CRS 19-24.

41. Daniel Patrick Moynihan, as quoted in Mark Perry, *Eclipse: The Last Days of the CIA* (New York, NY: William Morrow and Company, 1992), 308. Hereafter cited as Perry, *Eclipse*.

42. "The Once and Future CIA", *New York Times*, 18 October 1991.

primarily on trying to discern the intentions of the Soviet Union and its leaders had overestimated the strength of the Soviet economy.[43]

In order to try to maintain absolute objectivity in its assessments of the Soviet Economy, CIA estimates relied heavily on numerical data. The most important calculation was the military-to-civilian spending ratio.[44] A flaw in its methodology became evident when the CIA assessed that the Soviet Union would have the capacity to continue both its military build-up and its aggressive foreign policy despite its clear economic problems.[45] Richard Kerr defended the agency's performance in a letter to the editor of the *New York Times,* stating, "the CIA has been saying with increasing insistence since the late 1980's that Mr. Gorbachev's policies of half-way reform would not work. In examining the likely result of this failure we posited scenarios ranging from reactionary retrenchment to a breakthrough by the democrats lead by Boris N. Yeltsin."[46]

Despite the claims by Kerr that the CIA was aware of the Soviet Union's problems, the Defense Department continued to assess that "the modernization of Soviet Strategic forces is going full steam, including the deployment of two new types of weapon, the SS-18 and a new generation of ICBMs."[47] Additionally, that year's *Soviet Military Power*, a glossy annual compendium of Soviet military activities published by the DoD, described Gorbachev's arms control initiatives as being designed to weaken NATO countries, increase tensions in US-Europe relations, put obstacles in the path of Western allies' defense plans and at the same time enable the Soviets to continue to develop their military might.[48]

Whether or not the CIA predicted the Soviet collapse is really immaterial. What is important to note is that the drive to satisfy the goals of the organization continued right up to its collapse, clearly demonstrated by the DoD's assessment of Soviet activity. However, the Cold War was ultimately a win for the United States, which probably

---

43. Perry, *Eclipse*, 308.

44. Ofira Seliktar, Politics, Paradigms, and Intelligence Failures: Why So Few Predicted the Collapse of the Soviet Union (Armonk, NY: M-E Sharpe Inc., 2004), 215.

45. David Arbel and Ran Edelist, Western Intelligence and the Collapse of the Soviet Union: 1980-1990 – Ten Years that did not Shake the World (Portland, OR: Frank Cass Publishers, 2003), 232.

46. Richard J. Kerr, Acting Director of Central Intelligence, "Letter to the Editor," *New York Times*, 24 October 1991.

47. Arbel and Edelist, *Western Intelligence*, 234.

48. Ibid.

explains why Congress did not call for an in depth investigation of the IC's performance leading up to the Soviet collapse. It would be unseemly to investigate an organization that played such a crucial part in holding the line against Soviet expansion for ineptitude. Unfortunately, this failure to investigate may have contributed to the intelligence failures that were to continue to plague the IC in the period immediately following the end of the Cold War.

Chapter 4

Post Cold War – The Broken System Continues

With the fall of the Soviet Union, the US moved from the Cold War to the Post-Cold War era. Despite a clear change in the geopolitical landscape, the problems that plagued the IC during the Cold War continued to affect its performance as it tried to deal with new problems and new threats.

This chapter presents a brief examination of the performance of the intelligence community in the early portions of the Post-Cold War era. It is focused upon three intelligence failures from this period to determine if the three posited reasons why the IC doesn't share information are still present, in roughly the same form as from its inception, and also to determine if these tendencies contributed to the failures. First examined is the performance of the IC during Operations Desert Shield and Desert Storm. I will comment on the IC's failure to warn policymakers of the impending Iraqi invasion of Kuwait, and highlight some of the critiques that were levied on the IC following the end of hostilities in Iraq. Next, I describe the intelligence community's poor performance leading up to the surprise Indian nuclear tests of 1998. Finally, I provide a unique perspective on the IC's apparent inability to assess Iraq's weapons-of-mass-destruction (WMD) programs prior to the US-led invasion of Iraq in 2003.

Desert Shield/Desert Storm

On 2 August 1990, Iraqi forces invaded Kuwait and quickly occupied the entire country. For all intents and purposes, the United States was surprised by the invasion. Whether or not the intelligence community provided warning to senior policymakers remains debatable.

The details of what the intelligence community provided prior to the invasion include:

- An early July report that indicates Iraqi troops are moving from the Iranian to the Kuwaiti border…movements are considered significant.
- 29 July, US surveillance detects the activation of an Iraqi radar system indicating war readiness.

- 31 July, US intelligence learns that Iraq is dispatching the requisites for a sustained attack to the Kuwaiti border – fuel, trucks, and cargo planes.
- 1 August, Secretary of State Baker tells Soviet Foreign Minister Eduard Shevardnadze that an invasion was imminent.[1]

In addition, Representative Robert G. Torricelli received an intelligence briefing from DIA analysts just 10 hours before the invasion. Torricelli said the intelligence reports showed that the United States "fully understood the potential of the Iraqi mobilization."[2] Other officials pointed out that even if the IC did provide *some* warning about the invasion, it occurred "too late for useful military or diplomatic deterrents."[3] Another criticism indicated that the CIA military assessments on Iraq were flawed, and pointed out that the agency initially assessed that Iraq's saber-rattling was bluster, not genuine.[4]

One thing is clear, however, and that is the US was not ready for the invasion. The State Department had not warned US citizens to leave Kuwait, and no advisories on travel to Kuwait had been issued. President Bush continued to prepare to travel to Aspen, Colorado the next day, as did Secretary of Defense Cheney, and the US is not believed to have offered military assistance to Kuwait or Saudi Arabia, although the US had an unstated agreement to defend its gulf allies if asked.[5]

Gregory Copley, in writing about the intelligence failure, said that the problem was not that key analysts in various intelligence agencies did not correctly assess that Iraq was going to invade Kuwait, but that this correct analysis "was not conveyed to national leaders in such a way as to induce correct policy decisions to be made."[6] According to Copley, some of the problems that contributed to the failure were: "an enormous concentration on collection, especially through technical means, a distinct lack of human intelligence (HUMINT) from clandestine sources, and too much raw information in the system."[7]

---

1. "Iraq Duped Everyone, except CIA," *USA Today*, 12 September 1990.
2. Robert G. Torrecilli, as quoted in David Hoffman, "US Misjudgment of Saddam Seen; Early Evidence of Bellicosity, Drive for Dominance Noted," *Washington Post*, 8 August 1990.
3. Michael Wines, "The Iraqi Invasion: U.S. Says Bush Was Surprised by the Iraqi Strike," *New York Times*, 5 August 1990.
4. Ibid.
5. Ibid.
6. Gregory Copley, "Intelligence and the Iraqi Invasion: Why Did So Many Services Fail," *Defense & Foreign Affairs' Strategic Policy* (September 1990), 38.
7. Ibid., 39.

One of the most outspoken critics of the intelligence community was the Commander in Chief of US Central Command, General H. Norman Schwarzkopf. His primary complaints concerned the IC's performance during Operations Desert Storm and Desert Shield, particularly in the way that the IC conducted bomb-damage assessment (BDA) of air strikes in Iraq. Following the war, Schwarzkopf told the Senate Armed Services Committee that conflict between the CIA, DIA, and other intelligence agencies over various Iraqi capabilities produced "major areas of confusion."[8] Schwarzkopf also told the Committee, "there were so many disagreements within the intelligence community … so many disclaimers that by the time you got done reading many of the intelligence estimates, no matter what happened, they would have been right. And that's not helpful to the guy in the field. It really isn't."[9]

Schwarzkopf points out in his autobiography, *It Doesn't Take a Hero*, that the problem with the BDA process was that the IC was trying to turn it into a science by spending billions of dollars on surveillance technology. This allowed analysts to collect hard evidence on an air strike, which meant that the analyst did not have to rely on the pilot's report, which the IC tended to not trust. Conflicts were inevitable. For example, although the IC claimed that the Baghdad power plant had not been destroyed, Schwarzkopf pointed out that the lights were out in Baghdad.[10] The difference of opinion led CENTCOM to develop an objective and subjective grading criteria for damage assessment that seemed to placate both sides of the argument. But the criticism of the IC remained.

India's Nuclear Test

In May 1998, India surprised the US and the world when it detonated three nuclear devices. The US Intelligence Community did not provide any warning of the impending tests. Senator Richard C. Shelby, Chairman of the Senate Select Committee on Intelligence, deemed this "a colossal failure of U.S. intelligence" and "the intelligence

8. General H. Norman Schwarkopf, as quoted in David A. Fulghum, "Key Military Officials Criticize Intelligence Handling in Gulf War," *Aviation Week & Space Technology*, 24 June 1991.

9. John A. Gentry, *Lost Promise: How CIA Analysis Misserves the Nation: An Intelligence Assessmen* (Lanham, MD: University Press of America, Inc., 1993), 160.

10. H. Norman Schwarkopf, General, USA (Ret), *It Doesn't Take A Hero*: *The Autobiography of General H. Norman Schwarzkopf* (New York, NY: Bantam Books, 1992), 430-432.

failure of the decade."[11] While Senator Daniel Patrick Moynihan asked, "why didn't the CIA find this out? What's the State Department for? The question is why don't we learn to read? The political leadership in India as much as said they were going to begin testing."[12]

When Senator Moynihan rhetorically asked why we don't learn to read, one can only assume that he was referring to the fact that the Bharatiya Janata Party (BJP) had openly campaigned that if elected it would "exercise the option to induct nuclear weapons."[13] From open-press reports alone, it should have not been surprising that India conducted the tests, especially considering that the BJP came to power via a minority coalition government in March 1998.

The investigation into the IC's failure to anticipate the Indian nuclear test was led by retired Admiral David Jeremiah, former vice chairman of the Joint Chiefs of Staff. His report, often referred to as the Jeremiah report, remains classified. However, the press conference he conducted following the submission of his report provides some insight into the findings. Jeremiah's bottom line was "that both the intelligence and the policy communities had an underlying mindset going into these tests that the BJP would behave as we behave. For instance there is an assumption that the BJP platform would mirror Western political platforms."[14] Jeremiah criticized the IC and the policy community for its belief that despite the BJP's pledge to conduct the tests, once it came to power it would decide to rule responsibility and not do so.[15] As Jeremiah pointed out, this was essentially a case of mirror imaging within both communities.

Jeremiah also called for a greater use of outside experts, both systematically and during periods of transition on a major intelligence issue. Jeremiah saw these two steps

---

11. Senator Richard Shelby, as quoted in Tim Weiner, "Nuclear Anxiety: The Blunders; U.S. Blundered on Intelligence, Officials Admit," *New York Times*, 13 May 1998. See also "U.S. Intelligence Failure Seen," 13 May 1998, on line, Internet 8 June 2005, available from http://www.cnn.com/WORLD/asiapcf/9805/13/india.cia.update/.

12. Senator Daniel Patrick Moynihan, as quoted in Weiner, "Nuclear Anxiety."

13. Richard A. Best, "US Intelligence and India's Nuclear Tests: Lessons Learned," *CRS Report for Congress*, 98-672, 11 August 1998, 2. See also "New Government in India Heightens Nuclear Concerns," *Disarmament Diplomacy*, no. 24, March 1998, n.p., on line, internet 6 July 2005, available from http://www.acronym.org.uk/dd/dd24/24new.htm.

14. David E. Jeremiah, Admiral, USN (Ret.), "Jeremiah News Conference," on line, internet 3 July 2004, available at http://www.odci.gov/cia/public_affairs/press_release/1998/jeremiah.html. Hereafter cited as the Jeremiah Report.

15. Walter Pincus, "Spy Agencies Faulted for Missing Indian Tests," *Washington Post*, 3 June 1998.

as a way to work against the "everybody thinks like us" mindset.[16] He called for increased management to oversee and integrate the IC's collection systems "so that we task collection as a 'system of systems' rather than each of the individual pipelines," and he called for the IC to develop the contrarian view as part of the IC's warning process.[17] When asked about compartmentation within the IC, Jeremiah responded that "compartmentation is an important issue. It is a requirement if you are going to continue to maintain your sources. But the issue really is how do I use this particular intelligence system to collect the data that allows me to target that system on a particular objective? And that coordination across the INTs, is the phraseology, has not been as clear and as clean as it should be. And I think that is the issue we want to try to get at."[18]

Iraq's WMD Programs

The IC's assessment that Iraq was working to reconstitute its WMD program was the primary reason given for the US-led invasion of Iraq in 2003. With its inability to substantiate claims of Iraqi WMD development with physical evidence, the IC was heavily criticized by two different investigations. The first was commissioned by the Senate Select Committee on Intelligence. Its output, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, concluded that, "Most of the major key judgments in the Intelligence Community's October 2002 National Intelligence Estimate (NIE), Iraq's Continuing Programs for Weapons of Mass Destruction, either overstated, or were not supported by, the underlying intelligence reporting. A series of failures, particularly in analytic trade craft, led to the mischaracterization of the intelligence."[19] The second investigation into the performance of the IC leading up to the US led invasion of Iraq was established by President Bush via Executive Order 13328 "Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction."[20] The Commission's assessment, usually

16. Jeremiah Report.
17. Ibid.
18. Ibid.
19. Senate Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, 108th Cong., 7 July 2004, 14. Hereafter cited as Senate WMD report.
20. Executive Order 13328, Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 6 February 2004. As found in The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the*

referred to as the Robb-Silberman report, found that the intelligence community was "dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction. This was a major intelligence failure … Its principal causes were the Intelligence Community's inability to collect good information about Iraq's WMD programs, serious errors in analyzing what information it could gather, and a failure to make clear just how much of its analysis was based on assumptions, rather than good evidence. On a matter of this importance, we simply cannot afford failures of this magnitude."[21] This section of this thesis relies heavily on these two investigations as both were extremely critical of the IC and both are extremely current.

During its investigation, the Senate's committee discovered that intelligence analysts from multiple agencies create 'finished' intelligence products derived from the same sources. The committee pointed out that "in an ideal situation, these analysts will be in regular contact over secure communications to discuss new information, to share ideas and to brainstorm about how the information can be presented to policymakers to best satisfy their requirements, however, this exchange does not always occur."[22] The committee also noted that while coordination of an intelligence product with the rest of the IC depended on the product itself, "in many instances, each agency produces its own finished products which are subject to review and editing by its own internal management." These finished products are then delivered to a number of different consumers, including "policy makers and warfighters."[23] Thus it seems that a single agency's products, while primarily intended for a specific customer or customers, will also be provided to the leadership of another branch or department of the government. For example, the Defense Intelligence Agency's finished intelligence products are primarily intended for the Secretary of Defense and the Secretary's staff, along with the senior leadership of the Joint Chiefs and the Commanders of the Unified Commands. But, DIA products are also delivered to the White House and to the State Department, without necessarily being coordinated with either the CIA or State/INR.

President (Washington D.C.: Government Printing Office, 31 March 2005), 551. Hereafter cited as the Robb-Silberman Report.

21. Ibid., letter of transmission.
22. Senate WMD Report, 7.
23. Ibid.

The Senate committee found another pertinent example for this thesis. One of the primary causes of a lack of sharing information is the CIA's overzealous protection of its human intelligence (HUMINT) sources; "the CIA continues to excessively compartment sensitive HUMINT reporting and fails to share important information about HUMINT reporting and sources with Intelligence Community analysts who have a need to know."[24] In this type of case, the need to protect the source of the information was considered by the CIA as more important than the need to share. As collector of the information, such tight control was completely within the agency's purview. But the Senate Committee also concluded that the CIA abused its position as the coordinator of the IC's activities by controlling "the presentation of information to policymakers, and exclud[ing] analysis from other agencies."[25] The Committee also found

> that significant reportable intelligence was sequestered in CIA Directorate of Operations (DO) cables, distribution of sensitive intelligence reports was excessively restricted, and CIA analysts were often provided with "sensitive" information that was not made available to analysts who worked the same issues at other all-source analysis agencies. These restrictions, in several cases, kept information from analysts that was essential to their ability to make fully informed judgments. Analysts cannot be expected to formulate and present their best analysis to policymakers while having only partial knowledge of the issue.[26]

During its investigation, the President's Commission found that IC "collectors retain a strong institutional bias against sharing operational information with analysts."[27] In an interview with NSA officials conducted on 14 July 2004, the Commission found that NSA does not like to share raw data with anyone outside of NSA.[28] This reluctance is based on the desire to protect the source of the information, so to ensure further exploitation. However, when the description of the source is so vague as to preclude the ability of an analyst to determine the source's reliability, or whether or not information comes from the same source, then the amount of credibility that goes with the information can become skewed.

---

24. Ibid., 26.
25. Ibid., 27
26. Ibid.
27. Robb-Silberman Report, 177
28. Ibid., 177 and 244, footnote 787.

The President's Commission, like the Senate's, also found that "individual departments and agencies continue to act as though they own the information they collect, forcing other agencies to pry information from them. Similarly, much information deemed 'operational' by the CIA and the FBI isn't routinely shared, even thought analysts have repeatedly stressed its importance."[29] To be sure, this lack of information sharing wasn't all one sided. "The systemic lack of effective information sharing occurs in the other direction as well, however. For example, the [CIA] DO was not aware that the [CIA] DI was relying so heavily on reporting from Curveball in its pre-war assessments of Iraq's BW program." Similarly, the Defense HUMINT official who was asked to coordinate on a speech that Secretary of State Powell was to give was not aware that the speech relied heavily on information that had come from a source the DIA officer knew to be a fabricator, and not some other source.[30]

Conclusion

As the Cold War came to a close, the IC, and especially the CIA, struggled to determine its new mission. After focusing on the Soviet Union for the past 40 years, it no longer had a reliable enemy on which to concentrate its efforts. This problem is especially evident in Director Robert Gates' statement before the Senate Select Committee on Intelligence. While discussing the CIA's support to the recent war effort, Gates said:

> CIA has basically been considered a fundamentally peacetime organization…But war then…was defined as something like global thermonuclear war…what the Gulf War showed, unlike Vietnam…was that in this intense, very large conventional war, we had something in between…peace and full scale war.
>
> We really didn't have, I think, very good procedures particularly for CIA support for military operations of that scale. I think that is one of the areas we need to look at…We discovered some real problems during the course of the war…in terms of the transmission of our information to local commanders, to the commanders on the ground.[31]

29. Ibid., 14.
30. Ibid., 179.
31. Senate, "Nomination of Robert M. Gates to be Director of the Central Intelligence Agency: Hearing of the Senate Intelligence Committee," 102nd Cong., 17 September 1991,

Presidential Decision Directive (PDD) 35, as set forth by President William Clinton, removed some of the ambiguity the IC was suffering when prioritizing assigned missions.[32] PDD-35 made intelligence support to military operations the primary mission of the IC. This was followed by political, economic, and military intelligence on countries hostile to the US, and, lastly, protecting American citizens from new trans-national threats including terrorists, organized crime, and weapons of mass destruction.[33] This change in priorities also provided the IC an excuse as to why it failed to predict the Indian Nuclear Test.

Throughout the post-Cold War period it seems the IC was searching for a reason to exist. Recalling the theory on why organizations are created, it is understandable that the agencies of the IC, and especially the CIA, were trying to find a continuing mission and thus justify their existence. Because organizations come into existence for a specific reason, and as it seemed that the reason for the CIA to exist, a strong and belligerent Soviet Union, had gone away, the CIA faced an identity crisis. This identity crisis resulted in the CIA searching for a mission through the early 1990s—until the President provided it with a primary requirement to support military operations.

One can only surmise that as each agency within the IC found new mission areas to exploit, and along with them new sources of information, that the lack of sharing problem increased. Not only was the mandate to carve out new mission area obvious, agencies felt additionally threatened by budget cuts that were also occurring during this period. Justifying one's existence in a period of downsizing does not make for a cooperative environment. This intensified lack of sharing carried forward to the US-led invasion of Iraq in 2003. Relying heavily on IC assessments for *causus belli*, it was only after US forces occupied the country that it learned the IC's assessment on Iraq's WMD program was utterly wrong. This clear failure led to investigations on behalf of both the Senate and the President.

Both investigations confirmed what had been surmised earlier; through the 1990s, the IC became more and more entrenched in protecting its sources. The reason for this

---

32. Walter Pincus, "Control Tightened on Spy Agencies; White House Sets Priorities for Intelligence Gathering," *Washington Post*, 10 March 1995.

33. William Jefferson Clinton, "Remarks by the President at the 50th Anniversary of the Central Intelligence Agency," 16 September 1997 , on line, internet 4 July 2005, available at http://www.fas.org/irp/offdocs/pdd35.htm.

entrenchment was twofold. First, each IC agency was protecting its *raison d'existence.* Second, each agency was protecting the information it collected in a way that presumed ownership of the information. Furthermore, two of the three explanations for investigations into this period in the history of the IC directly support why IC agencies don't share information: the nature of the organization, and the nature of the information.

The next chapter focuses solely on the events leading up to the terrorist attacks on 11 September 2001. The failure of the IC to properly assess the decades-long Iraqi WMD effort was not known until after the terrorist attacks of that fateful day, but it was the intelligence failures associated with the attack on US soil that proved to be the break point in tolerating the IC's ambiguous post-Cold War legacy. The subsequent investigation provided the catalyst necessary to bring about significant change in the intelligence community.

Chapter 5

11 September 2001 – The Last Straw

At 0846:40 EDT, 11 September 2001, American Airlines flight 11 from Boston to Los Angeles crashed into the North tower of the World Trade Center. Sixteen minutes and 31 seconds later, United Airlines flight 175, also from Boston to Los Angeles, struck the South tower of the World Trade Center. At 0937:46 on the same morning, American Airlines flight 77, from Washington D.C. to Los Angeles, crashed into the Pentagon. And finally, at 1003:11 United Airlines Flight 93, from Newark to San Francisco, crashed into a field in Shanksville, Pennsylvania, brought down short of its target as the passengers on board revolted against the hijackers.[1]

The sequence of events on this fateful day shocked the United States. It has been called the worst foreign attack on American soil in US history, and an intelligence failure of monumental proportions. It was inevitable that there be an investigation. The National Commission on Terrorist Attacks upon the United States was the investigative body. Its final report is entitled *The 9/11 Commission Report*.

This chapter is focused exclusively on the investigations into the events leading up to the 9/11 attack. As such, this chapter relies heavily on the 9/11 Commission's investigation, its findings, and its conclusions, as well as the Joint Inquiry into the Terrorist Attacks of September 11, 2001. The main reason for the heavy reliance on these two sources is the fact that significant portions of both of these reports' findings, conclusions, and recommendations were incorporated into the Intelligence Reform and Terrorism Prevention Act of 2004, which became law on 17 December 2004.[2] In addition, the investigations are the most complete and reliable sources on the events to date.

---

1. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report.* Official Government Edition (Washington D.C.: U.S. Government Printing Office, 2004), 32-33. Hereafter cited as the 9/11 Commission Report,

2. *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-458, 108th Cong. (17 December 2004), 1.

One of the first things that stands out in reading the 9/11 Commission report is that it seems the IC was not sure of the kind of threat posed by Usama Bin Ladin and al Qaeda. Although al Qaeda was formed in 1988, the IC did not describe the organization until 1999, despite the fact that the IC had received information that Bin Ladin was in charge of his own terrorist organization "with its own targeting agenda and operational commanders" in 1996-97.[3] Neither the 1995 nor 1997 National Intelligence Estimate made any significant references to Bin Ladin.

Information did begin to come forth starting in 1999, and a number of intelligence reports were prepared for the highest officials in Washington on different issues surrounding Bin Ladin, his political philosophy, and his desire to target the United States. However, "there were no complete portraits of his strategy or of the extent of his organization's involvement in past terrorist attacks. Nor had the intelligence community provided an authoritative depiction of his organization's relationships with other governments, or the scale of the threats his organization posed to the United States."[4]

Though ultimately inadequate, the US intelligence community had taken steps to increase its analytic capability against terrorism prior to the 9/11 attacks. For example, a 1986 task force on international terrorism chaired by Vice President Bush "concluded that US Government agencies collected information on terrorism but did not aggressively operate to disrupt terrorist activities."[5] In response to this finding, the Director of Central Intelligence created the DCI Counterterrorist Center (CTC) with the mission to assist the Director of Central Intelligence in coordinating the counterterrorist efforts of the Intelligence Community by

- Implementing a comprehensive counterterrorist operations program to collect intelligence on and minimize the capabilities of, international terrorist groups and state sponsors.
- Exploiting all-source intelligence to produce in-depth analyses of the groups and states responsible for international terrorism
- Coordinating the Intelligence Community's counterterrorist activities.[6]

---

3. 9/11 Commission Report, 341.

4. Ibid., 342.

5. Central Intelligence Agency, *DCI Counterterrorist Center*, n.p., on-line, internet 29 May 2005, available from http://www.cia.gov/terrorism/ctc.html

6. Ibid.

In this way, the CTC became the analytic center for the intelligence community's counterterrorism efforts. Following the 1993 bombing of the World Trade Center, and as information became available concerning Usama Bin Ladin and his terrorist activities, the CTC created a special unit to focus on Bin Ladin and his associates. This unit "became the hub for expertise on Bin Ladin and for operations directed against his terrorist network, al Qaida."[7]

While the CTC's analytic output, according to Deputy DCI John McLaughlin, "dramatically eclipsed" any analysis that might have been done via a National Intelligence Estimate prior to the 9/11 attack, the CTC's work focused primarily on collection issues.[8] Recognizing shortfalls in strategic analysis, DCI George Tenet created a new strategic assessments branch within the CTC in July 2001. Although the decision to add an additional ten analysts to this effort "was seen as a major bureaucratic victory, the CTC labored hard to find them. The new chief of this branch reported for duty on 10 September, 2001."[9]

Staffing for the CTC was supplied primarily by CIA, although the Departments of State, Transportation, Treasury, Energy, the INS, Customs, and others detailed personnel to the CTC.[10] The CTC and the FBI had also exchanged senior-level officers to help manage the counterterrorist efforts at both agencies.[11] Historically, however, people were brought into the CTC on a rotational basis. They would be assigned to the CTC for two years and then go back to their home office.[12]

Providing employees from one agency to another is often praised as a way to create personal relationships that facilitate information sharing between the agencies. This practice, however, assumes that those detailed will have the same level of access as

---

7. Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001. Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, Together with Additional Views, 7 July 2004, on-line, Internet 29 May 2005, available from http://www.gpoaccess.gov /serialset/creports/911.html. Hereafter cited as the Joint Inquiry.

8. John McLaughlin, interview with 9/11 Commission, 21 January 2004. as found in 9/11 Commission Report, 342.

9. Ibid.; and also Patti Kindsvater interview, 12 September 2003, as found in 9/11 Commission Report, 342.

10. Joint Inquiry, 362

11. Office of the Director of Central Intelligence, *DCI Counterterrorist Center,* on line, internet, available at http://www.odci.gov/terrorism/ctc.html

12. Joint Inquiry, 340.

if they were still assigned to the parent organization, as well as the same level of access to the information of the host agency as any other employee of that agency. Unfortunately, this is not always the case. Congress' Joint Inquiry into the Terrorist Attacks of September 11, 2001, found that host agencies often restrict access to information that detailees can query, and that oft times the detailee only learns about intelligence after "host agency employees make ad hoc judgments to share information."[13] This finding supports two of the theories put forth in this thesis. The unwillingness of a host organization to share information with someone from another agency demonstrates a desire to protect the agency or organization itself and the desire to protect the information. It is interesting to note however; that the Joint Inquiry staff found that information was shared at the interpersonal level.

If there is any central theme to the 9/11 Commission Report it is probably this: "the biggest impediment to all-source analysis – to a greater likelihood of connecting the dots – is the human or systemic resistance to sharing information."[14] One only need look at the list of Operational Opportunities found in the 9/11 Report to see examples of the IC not sharing information:

1. January 2000: the CIA does not watchlist Khalid al Mihdhar or notify the FBI when it learned Mihdhar possessed a valid US visa.
2. March 2000: the CIA does not watchlist Nawaf al Hazmi or notify the FBI when it learned that he possessed a US visa and had flown to Los Angeles on 15 January 2000.
3. January 2001: the CIA does not inform the FBI that a source had identified Khallad, or Tawfig bin Attash, a major figure in the October 2000 bombing of the USS Cole, as having attended the meeting in Kuala Lumpur with Khalid al Mihdhar.
4. May 2001: a CIA official does not notify the FBI about Mihdhar's US visa, Hazmi's US travel, or Khallad's having attended the Kuala Lumpur meeting (identified when he reviews all of the relevant traffic because of the high level of threats).
5. June 2001: FBI and CIA officials do not ensure that all relevant information regarding the Kuala Lumpur meeting was shared with the Cole investigators at the 11 June meeting.
6. August 2001: the FBI does not recognize the significance of the information regarding Mihdhar and Hazmi's possible arrival in the US and thus does not take action to share information, assign resources, and give sufficient priority to the search.

13. Joint Inquiry, 362.
14. 9/11 Commission Report, 416

7. August 2001: FBI headquarters does not recognize the significance of the information regarding Moussaoui's training and beliefs and thus does not take adequate action to share information, involve higher-level officials across agencies, obtain information regarding Moussaoui's ties to al Qaida, and give sufficient priority to determining what Moussaoui might be planning.[15]

These missed operational opportunities demonstrate how the CIA and FBI bureaucracies protect their information. The CIA was focusing on a terrorist organization overseas. It seemed to not have occurred to CTC analysts that al Qaida was planning an attack in the United States. As such, it treated the information it had as a foreign intelligence problem, and did not deem it necessary to share it with any other agency. The FBI, on the other hand, treated the information it had as though it was going to be used to support legal action against an individual. This is the routine manner with which it handles such information, and it probably never dawned on the FBI that the information may have been of critical value to others. These examples support the case of organizations not sharing information based on Allison and Zelikow's Model II behavior.

These obvious missed operational opportunities aren't the only examples of the IC not sharing information. "During 1999, NSA obtained a number of communications – none of which included specific details regarding the time, place, or nature of the September 11 attacks – connecting individuals to terrorism who were identified, after September 11, 2001, as participants in the attacks that occurred on that day."[16] In his testimony before the Joint Inquiry, Lieutenant General Mike Hayden, NSA Director, admitted that "we did not disseminate information we received in early 1999 that was unexceptional in its content, except that it associated the name of Nawaf Al-Hazmi with al Qaida."[17]

The performance of the IC in the days and years leading up to the 9/11 attack is consistent with the theories laid out in chapter 2 of this thesis. Both the FBI and the CIA have a role in preventing terrorism. The CIA's focus has traditionally been on terrorist activity and threats of terrorist attacks on US interests outside the United States. The FBI

15. 9/11 Commission Report, 355-356

16. Joint Inquiry, 11

17. Lt Gen Mike Hayden, as quoted in Bill Gertz, *Breakdown: The Failure of American Intelligence to Defeat Global Terror (*New York, NY: Penguin Group, 2003), 140.

on the other hand, focuses predominantly on the threat of a terrorist attack inside the US. Both organizations have routines and processes for dealing with threat information that work well within the agencies. But when the threat crossed the lines of authority between the two agencies, breakdowns began to occur.

NSA suffered from this same problem. By law, NSA is not allowed to deliberately collect data on US citizens or on persons in the United States without a warrant based on foreign intelligence requirements.[18] Because of this, NSA adopted a policy that avoided intercepting communications between individuals in the US and foreign countries even though the individuals in the US were communicating with known Middle East terrorist camps. NSA believed that the FBI was responsible for conducting this surveillance. However, neither the NSA nor the FBI developed a plan to ensure this kind of information was disseminated to the appropriate domestic agency.[19]

The performance of NSA also provides some insight into how the nature of intelligence information had changed. During World War II and through the early years of the Cold War, information provided by NSA and its forbearers was considered so sensitive that it was protected with the very highest levels of security. This meant that the dissemination of the information was also extremely restricted, but it was disseminated none the less. The decision by NSA not to disseminate a report that it considered unexceptional seems to indicate that the nature of information had changed. It was no longer necessary for NSA to disseminate all the information it had collected – rather NSA had decided it would only disseminate the information that it deemed important without necessarily knowing what the other members of the IC thought was important. Thus, it seems that NSA was willing to share; it just didn't know *what* to share.

The CTC's performance prior to 9/11 further shows how individuals within a group tend to behave in self rather than the group interest. When the 9/11 Commission asked who had the job of managing the case to make sure things were done, the CIA Deputy Director for Operations replied that the CTC was supposed to manage all the moving parts, while what happened on the ground was the responsibility of the managers

18. 9/11 Commission Report, 87.
19. Joint Inquiry, 36.

in the field.[20] However the CTC never really took responsibility for the case, and the director of the al Qaida unit in the CTC "did not think it was his job to direct what should or should not be done." Thus the CTC failed to perform its mission at two different levels of organization. In assessing its overall performance, the 9/11 Commission was very critical of the CTC's, highlighting that the CTC failed to analyze the telltale signs of an impending attack, and to use its imagination to anticipate what could occur:

1. The CTC did not analyze how aircraft, hijacked or explosives laden, might be used as a weapon. And thus determine the critical constraint for the terrorists—finding a suicide operative able to fly large jet aircraft.
2. The CTC did not develop a set of indicators for this method of attack.
3. The CTC did not propose, and the intelligence community collection management process did not set, requirements to monitor for such telltale indicators.
4. Neither the IC nor aviation security experts analyzed systemic defenses within an aircraft or against terrorist-controlled aircraft, suicidal or otherwise.[21]

The failure of the CTC may have been in part the result of how the members of the CTC interacted. Being correct is not often rewarded, but being wrong is almost always punished. Specifically in this case, there may have been a perceived risk in any individual putting forth the idea that a terrorist might use an aircraft as a weapon vice just hijack it for political purposes.

The 9/11 Commission came to the conclusion that "the 9/11 attacks revealed four different kinds of failures: in imagination, policy, capabilities, and management."[22] Three of these findings relate directly to the performance of the intelligence community. In the case of imagination the primary failure was the IC's inability or unwillingness to preconceive of the use of a hijacked aircraft as a weapon. In the area of capabilities the 9/11 Commission pointed out that the US tried to solve the al Qaida problem using the same governmental institutions and capabilities it had used during the last stages of the Cold War. This was especially true for the intelligence community and these institutions were insufficient. Finally, in the case of management intelligence information was not shared, and analysis was not pooled. As the Commission pointed out "the agencies are

20. James Pavitt interview, 8 January 2004, as found in 9/11 Commission, 355-356.
21. 9/11 Commission 347.
22. Ibid., 339.

like a set of specialists in a hospital, each ordering tests, looking for symptoms, and prescribing medications. What is missing is the attending physician who makes sure they work as a team."[23]

The 9/11 Commission provided some recommendations as to how the IC could be structured in order to facilitate information sharing. Its first recommendation was the creation of a Director of National Intelligence (DNI) "to oversee national intelligence centers on specific subjects of interest across the US government and to manage the national intelligence program and oversee the agencies that contribute to it."[24] In essence, the 9/11 Commission recommended that the existing IC agencies become the military equivalent of the "organize, train, and equip" function for the IC, and that new National Intelligence Centers become the "Unified Commands" within the IC.[25]

The 9/11 Commission also stressed the IC develop and promote a "need-to-share" culture vice the "need-to-know" one that was in place. The recommendation lacked depth, however. Its only specific advice was to call for a horizontal approach to sharing based on a trusted-information network as put forth by the Markle Foundation.[26] Still the revamping of the IC has begun.

Conclusion

On 17 December 2004, President Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004, making it Public Law 108-458. This law created the position of Director of National Intelligence and tasked the Director to ensure the "maximum availability of and access to intelligence information within the intelligence community."

On 17 February 2005, President Bush nominated Ambassador John D. Negroponte to be the first Director of National Intelligence in the country's history.[27] On 21 April 2005, the Senate confirmed Negroponte as the first Director of National

23. Ibid., 353.
24. Ibid., 411.
25. Ibid., 412.
26. Ibid., 418.
27. Douglas Jehl and Elisabeth Bumiller, "Bush Picks Longtime Diplomat for New Top Intelligence Job," *New York Times*, 18 February 2005.

Intelligence in US history.[28] This critical restructuring, with its emphasis on combined agency interaction and intelligence sharing is so significant it has some observers calling it the Goldwater-Nichols Act of the intelligence community.[29] The first move toward having the IC share more information has been made.

28. Scott Shane, "Negroponte Confirmed as Director of National Intelligence," *New York Times*, 22 April 2005.

29. Senate, Committee on Homeland Security and Government Affairs, "Lieberman Statement on Negroponte Confirmation," *Press Release*, n.p., on line, internet 5 July 2005, available from http://www.senate.gov~gov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=975&Month=4&Year=2005.

Chapter Six

Conclusions and Recommendations

That the intelligence community has shown—and continues to show—a propensity to not share information is hardly a revelation. Precisely why the IC does not share information, despite a common interest in providing the best quality assessments to decision makers and general knowledge of how to do so, is the meaningful question to which this thesis is directed. Three theoretical frameworks were proposed in order to structure the attempt to answer this question. First, that the IC doesn't share because of the way governmental organizations act and interact in order to protect the interests and objectives of the agency. Second, that the IC doesn't share because of the nature of the information with which the IC works. And, third, that the IC doesn't share information due to the problems inherent in the collective action approach to problem solving. Of these three theories, the two most often encountered were the governmental organizations model and the nature of the information with which the IC works.

The history of the intelligence community demonstrates the infighting that occurred among its many constitutive agencies as it was created and evolved. At almost every juncture, the unwillingness of the different bureaucratic organizations to cede information at the risk of losing control was plainly evident.[1] Both the State Department and the agencies that would eventually fall under the new Department of Defense fought the creation of the Coordinator of Information, the Central Intelligence Group, and the Central Intelligence Agency. Then, when the CIA became a *fait accompli*, both worked to ensure that a body on which they sat (and which provided them the ability to protect their interests) would oversee the activities of the CIA.

The Cold War history also revealed organizational changes to the IC that, while intended to create more efficient organizations, provided these new organizations the ability to control information, thus impeding information flow across the IC. Two examples were the creation of the National Security Agency and the National

1. For a more detailed discussion of the creation of the CIA see Amy B. Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999).

Reconnaissance Organization. Both was intended to facilitate information flow. NSA was created to break down the barriers between all three armed service's signals intelligence organizations as well as refocus their efforts on supporting the military as a whole vice the independent service. NRO was created to minimize the infighting that was occurring between the CIA and the Air Force as both organizations tried to gain control of the nation's satellite reconnaissance programs. In both cases, however, the organization that was created became an additional member of the IC bureaucracy that had the inherent ability to control access to the information it collected.

Organizational problems continued to plague the IC following the collapse of the Soviet Union, especially as the CIA and the IC as a whole searched to find a new mission. The search seems to have hampered the IC's performance leading up to and through Operations Desert Shield and Desert Storm, as evidenced by the criticism it received from a variety of quarters. Once the IC was provided a new mission—support to military operations, it seems that some of the other traditional missions fell by the wayside. Indeed, the directed focus on military operations is one of the excuses that have been offered as to why the IC did not provide any warning about India's nuclear tests in 1998.

It is clear that the organizational problems continued into the twenty-first century, as evidenced by the findings of both the Senate Select Committee on Intelligence and the Presidential investigations into the performance of the IC in assessing Iraq's WMD programs. The lack of information sharing both across and within the different agencies demonstrated the unwillingness of organizations to share information. The investigations also reveal something about the nature of the information with which the IC routinely works.

The IC failures leading up to the Japanese attack on Pearl Harbor, and the surprise North Korean attack into South Korea, have been attributed to the inability of SIGINT agencies of the time to work together, due in large part to the nature of bureaucracies, but also due to the sensitive nature of the information involved. The desire to protect the sources and methods by which information is collected is understandable, but the desire to protect may also create an inherent unwillingness to share. This unwillingness to share is not only associated with the SIGINT organizations. The Central Intelligence Agency's

Directorate of Operations has been heavily criticized for its overzealous protection of sources.

The nature of the information is changing however, as demonstrated by Lieutenant General Hayden's testimony before the 9/11 commission on the reason certain terrorist information was not disseminated. Hayden claimed it was not because the information was sensitive and needed protection, but that the information was deemed unexceptional, and therefore not important enough for dissemination. This statement indicates two phenomena: first, that the amount of information may be growing beyond the IC's ability to analyze it, and second, that the mindset on disseminating information has changed, but not necessarily for the better. On the latter point, since NSA did not know who might have needed this unexceptional bit of information, rather than provide it anyway, it chose to withhold the information on the assumption that it was not needed. This is a perverse form of the need-to-know principal in reverse. In this case, it wasn't that another individual or agency was denied access to the information; it was NSA deciding *a priori* that no one needed to know the information.

There is little evidence of the problems of group dynamics contributing to the lack of information sharing within the intelligence community, other than from the performance of the Counterterrorism Center prior to the 9/11 terrorist attack. Primarily, the CTC was heavily criticized for its lack of analytic imagination in anticipating those events. Although there are few if any details as to the work environment within the CTC, one can presume that the transient nature of the employees' service made it a less than ideal environment for fostering free, or outside the box thinking.

Thus, of the three theories provided as to why the IC doesn't share information, the two that weigh the heaviest on the IC seem to be the bureaucratic organization of the IC and the nature of the intelligence information with which the intelligence community works. It is these two primary problems that the following recommendations address.

Recommendations

The first problem the DNI should take up is the dichotomy of need-to-know versus need-to-share. Another way to view this problem is through the lens of information ownership. As long as the collecting agency has the ability to classify the

information it collects in accordance with its own rules and regulations, information will not be efficiently shared. To this end, the Director of National Intelligence should empower a panel of experts to establish common security standards across the intelligence community. While there does not have to be one single standard for all, there does need to be commonality. In this way any individual cleared for A,B, and C in one agency is cleared for A, B, and C in all agencies, and that individual should have access to all the information that is classified A, B, and C.

Another way to foster the sharing of information would be to create a central repository for all finished intelligence products. This repository should be accessible by all members of the intelligence community at an appropriate classification level. Included with this central repository should be the contact information of the office that created the report. Responsibility for the product needs to remain with the office due to the practice of moving analysts from place to place.

Organizationally, the Intelligence Reform and Terrorism Prevention Act of 2004 is intended to do for the intelligence community what the 1986 Goldwater-Nichols Act did for the Department of Defense—promote cooperation and "jointness."[2] One of the primary results of this act was to make the armed services responsible for the training, organizing, and equipping of the service while the geographical and functional unified commands were responsible for employing these armed forces in a unified manner. [3] The analogy is used because of the authority that the Intelligence Reform and Terrorism Prevention Act of 2004 gives to the Director of National Intelligence to establish both functional and regional intelligence centers.[4] In this case the national intelligence centers become the "unified commands" of the intelligence community, while the agencies that traditionally make up the IC become the "armed services" responsible for the organize, train, and equip function. The problem this analogy highlights, however, is that the

---

2. Senate, Committee on Homeland Security and Government Affairs, "Lieberman Statement on Negroponte Confirmation," *Press Release*, n.p., on line, internet 5 July 2005, available from http://www.senate.gov~gov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=975&Month=4&Year=2005.

3. For the Goldwater-Nichols Act see Public Law 99-433. For a general discussion of the act see Gordon Lederman, *Reorganizing the Joint Chiefs of Staff: The Goldwater-Nichols Act of 1986* (Westport, CT: Greenwood Press, 1999), and James Locher, *Victory on the Potomac: The Goldwater-Nichols Act Unifies the Pentagon* (College Station, TX: Texas A&M University Press, 2002).

4. *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-458, 108th Cong. (17 December 2004), sec 1023.

agencies do more than just organize, train, and equip. They also collect, analyze, and report, thus their functions will overlap with the centers. Hence, the problem with the analogous national intelligence centers concept is that the analysts that staff the centers will continue to be provided by the existing agencies, and these employees will continue to fall under the rules (including pay and promotion) of their parent organization. One way to address this problem is by funding the national centers as independent organizations, an option the new DCI should take under careful consideration.

By funding the national intelligence centers directly, and allowing them to hire their own employees, the problem of having individuals that owe allegiance to an outside organization is removed. This funding will allow the centers the flexibility they need to maintain a viable and efficient work force while at the same time providing greater opportunity for the employees within the IC (and individuals outside it) who have regional or functional areas of expertise. The national centers should be billed as analytic centers of excellence, and incentives should be provided to foster the desire of individual analysts to work there. Employment at the centers could be considered a jumping off point for additional authority and responsibility back at the individual's home agency; however, it should not be necessary for individuals to return to their home agencies if there are opportunities elsewhere.

Providing funding to the centers would also allow the centers to contract with outside experts to provide consulting and educational services to the center itself. These outside experts could come from industry or academia. By establishing these kinds of relationships, the centers would be fostering an environment that would allow an analyst the opportunity to leave the IC for a time to gain further education or experience, and then either to return to or consult with the IC. The key is that this is done via the intelligence centers, and not through the traditional agencies.

Implementing these two recommendations will go a long way to addressing the basic causes for the intelligence community's predilection against sharing intelligence information. These recommendations should remove the ability of the agencies to classify information as they see fit, and by funding the centers the ties that the individual analyst had to his or her parent agency are broken, thus ensuring that as the center achieves its goals and objectives, the employees of the center benefit as well.

Bibliography

Allison, Graham and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis.* Second edition. New York, Addison-Wesley Educational Publishers, Inc., 1999.

Andrew, Christopher. "Codebreakers and Foreign Offices." In *The Missing Dimensions: Governments and Intelligence Communities in the Twentieth Century.* Edited by Christopher Andrew and David Dilks. London: Macmillan, 1984.

Andrew, Christopher. For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush. New York, NY: HarperPerrennial, 1995.

Arbel, David and Ran Edelist. Western Intelligence and the Collapse of the Soviet Union: 1980-1990 – Ten Years that did not Shake the World. Portland, OR: Frank Cass Publishers, 2003.

Armistead, Leigh, ed. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington D.C.: Brassey's, Inc., 2004.

Bamford, James. The Puzzle Palace: A Report on America's Most Secret Agency. New York, NY: Penguin Books, 1982.

Beschloss, Michael R. *The Crisis Years: Kennedy and Khrushchev, 1960-1963.* New York, NY: Edward Burlingame Books, 1991.

Best, Richard A. "US Intelligence and India's Nuclear Tests: Lessons Learned." *CRS Report for Congress,* 98-672, 11 August 1998.

Best, Richard A. Jr., "Proposals for Intelligence Reorganization, 1949-1996." As found in House, Permanent Select Committee on Intelligence. *IC21: Intelligence Community in the 21st Century*, Appendix C. Washington, D.C.: U.S. Government Printing Office, 1996.

Brownell, George. *The Origin and Development of the National Security Agency.* Laguna Hills, CA: Aegean Park Press, 1981.

Brugioni, Dino A. Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis. New York: Random House, 1991.

Central Intelligence Agency. *DCI Counterterrorist Center.* On-line. Internet, 29 May 2005. Available from http://www.cia.gov/terrorism/ctc.html.

Cline, Ray. *The CIA Under Reagan, Bush, and Casey.* Washington: Acropolis Books, 1981.

Clinton, William Jefferson. *Remarks by the President at the 50th Anniversary of the Central Intelligence Agency*, 16 September 1997. On line. Internet, 4 July 2005. Available from http://www.fas.org/ irp/offdocs/pdd35.htm.

Commission on Organization of the Executive Branch of the U.S. Government (1953-1955), *Intelligence Activities: A Report to the Congress*, 84th Cong, H. Doc. 201.

Copley, Gregory. "Intelligence and the Iraqi Invasion: Why Did So Many Services Fail," *Defense & Foreign Affairs' Strategic Policy* (September 1990): 38-42.

Dahl, Robert. *Who Governs?* New Haven: Yale University Press, 1961.

Denning, Dorothy E. *Information Warfare and Security.* New York, ACM Press, 1999.

Department of Defense Directive S-5100.20, "The National Security Agency and the Central Security Service," 23 December 1971. Previously declassified.

Department of Defense Directive TS 5105.23. "(S) National Reconnaissance Office," 27 March 1964. Previously declassified.

Department of Justice. *Report on CIA-Related Electronic Surveillance Activities.* Washington D.C.: Department of Justice, 1976.

Director of Central Intelligence. *DCI Counterterrorist Center.* On line. Internet, 25 May 2005. Available from http://www.odci.gov/terrorism/ctc.html

Director of Central Intelligence. *DCID 1/7*. Online. Internet 25 January 2005. Available from https://ia.gordoin.army.mil/ iaso/DCID/17/dcid1-7.html.

Dulles, Allen W., Mathias F. Correa, and William H. Jackson. *The Central Intelligence Organization and National Organization for Intelligence*. On-line. Internet, 30 June 2005. Available from http://www.state.gov/ www/about_state/history/ intel/350_359.html.

Eberstadt, Ferdinand. *National Security Organization*, Appendix G. Washington D.C., US Government Printing Office, 1949.

"The Economics of Sharing." *Economist*, 5 February 2005.

Etzioni, Amitai. *Modern Organizations.* Englewood Cliffs, NJ: Prentice-Hall Inc., 1964.

Executive Order 13328, Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 6 February 2004.

Fulghum, David A. "Key Military Officials Criticize Intelligence Handling in Gulf War." *Aviation Week & Space Technology*, 24 June 1991.

Gentry, John A. Lost Promise: How CIA Analysis Misserves the Nation: An Intelligence Assessment. Lanham, MD: University Press of America, Inc., 1993.

Gertz, Bill. Breakdown: The Failure of American Intelligence to Defeat Global Terror. New York, NY: Penguin Group, 2003.

Hoffman, David. "US Misjudgment of Saddam Seen; Early Evidence of Bellicosity, Drive for Dominance Noted." *Washington Post*, 8 August 1990.

Hoffman, L.R. "Conditions for Creative Problem Solving." *Journal of Psychology* 52, (1961): 429-444.

Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 108th Cong. (17 December 2004).

"Iraq Duped Everyone, except CIA." *USA Today*, 12 September 1990.

Janis, Irving L. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes.* Second edition. Boston, MA: Houghton Mifflin Company, 1982.

Jehl, Douglas and Elisabeth Bumiller. "Bush Picks Longtime Diplomat for New Top Intelligence Job." *New York Times*, 18 February 2005.

Jeremiah, David E., Admiral, USN (Ret.). Jeremiah News Conference. On line. Internet 3 July 2004. Available from http://www.odci.gov/cia/public_affairs/press_release/1998/jeremiah.html.

Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001. Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, Together with Additional Views. On-line. Internet, 29 May 2005. Available from http://www.gpoaccess.gov/serialset/creports/911.html. .

Kerr, Richard J. "Letter to the Editor." *New York Times*, 24 October 1991.

Khan, David. "Roosevelt, MAGIC, and ULTRA." *Cryptologia*, 14 (1992): 14-35.

Kuehl, Dan. "Foreword." In *Information Operations: Warfare and the Hard Reality of Soft Power*. Edited by Leigh Armistead. Washington D.C.: Brassey's, Inc., 2004.

Lederman, Gordon. Reorganizing the Joint Chiefs of Staff: The Goldwater-Nichols Act of 1986. Westport, CT: Greenwood Press, 1999.

Locher, James. *Victory on the Potomac: The Goldwater-Nichols Act Unifies the Pentagon*. College Station, TX: Texas A&M University Press, 2002.

Lowenthall, Mark M. *Intelligence: From Secrets to Policy*. Second edition. Washington D.C.: CQ Press, 2003.

Maier, Norman R. F. "Assets and Liabilities in Group Problem Solving: The Need for an Integrative Approach." In *Classics of Organizational Behavior*. Edited by Walter E. Natemeyer. Oak Park, IL: Moore Publishing Company, Inc., 1978.

Manning, Alan. *Monopsony in Motion: Imperfect Competition in Labor Markets.* New Haven, CT: Yale University Press, 2005.

March, James G. A Primer on Decision Making: How Decisions Happen. New York: Free Press, 1994.

March, James G. and Herbert A. Simon, *Organizations*. Second edition. Cambridge: Blackwell Publishers, 1993.

Markle Foundation, *Task Force on National Security in the Information Age*. On-line. Internet, 26 June 2005. Available from, http://www.markletaskforce.org/about.html.

Marx, Karl. "The Two Factors of a Commodity: Use-Value and Value." In *Social Theory: The Multicultural and Classic Readings*. Second edition. Edited by Charles Lemert. Boulder, CO: Westview Press, 1999.

Mill, John Stuart. System of Logic Rational and Deductive: Being a Connected View of the Principles of Evidence and the Methods of Scientific Investigation. London: Longman's, 1864. Book III, Chapter VIII.

Moe, Terry M. "The Politics of Bureaucratic Structure." In *Can the Government Govern?* Edited by John Chubb and Paul Peterson. Washington, DC; Brookings Institution, 1989.

Morgan, Gareth. *Images of Organization*. Second edition. Thousand Oaks, CA: Sage Publications, 1997.

Morganthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace.* New York: Alfred A. Knopf, 1967.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report.* Official Government Edition. Washington D.C.: U.S. Government Printing Office, 2004.

National Security Agency/Central Security Service. *NSA/CSS Manual 22-1*. Ft. Meade.: NSA 1986.

National Security Cryptologic Intelligence Directive No. 6. "Signals Intelligence." 17 February 1972.

"New Government in India Heightens Nuclear Concerns." *Disarmament Diplomacy*, no. 24, (March 1998). On line. Internet, 6 July 2005. Available from http://www.acronym.org.uk/dd/dd24/24new.htm.

NSC Intelligence Directive No. 12. "Avoidance of Publicity Concerning the Intelligence Agencies of the U.S. Government," 6 January, 1950.

Nye, Joseph S. Jr., Power in the Global Information Age: From Realism to Globalization. New York, NY: Routledge, 2004.

Olson, Mancur. The Logic of Collective Action: Public Goods and the Theory of Groups. Cambridge, MA: Harvard University Press, 1971.

"The Once and Future CIA." *New York Times.* 18 October 1991.

Parsons, Talcott. *Structure and Process in Modern Societies.* Glencoe, IL: The Free Press, 1960.

Perry, Mark. *Eclipse: The Last Days of the CIA.* New York, NY: William Morrow and Company, 1992.

Pincus, Walter. "Control Tightened on Spy Agencies; White House Sets Priorities for Intelligence Gathering." *Washington Post*, 10 March 1995.

Pincus, Walter. "Spy Agencies Faulted for Missing Indian Tests." *Washington Post*, 3 June 1998.

Prjeworski, Adam, and Henry Teune. *The Logic of Comparative Social Inquiry*. Melbourne, FL: Krieger, 1982.

Richelson, Jeffrey T. *The US Intelligence Community*. Fourth edition. Boulder, CO: Westview Press, 1999.

Schlesinger, James R. "A Review of the Intelligence Community, March 10, 1971." On line. Internet, 25 Jan 2005. Available from http://www.gwu.edu/~nsarchiv/ NSAEBB/NSAEBB144/ document%202.pdf.

Schwarkopf, H. Norman, General, USA (Ret). *It Doesn't Take A Hero: The Autobiography of General H. Norman Schwarzkopf.* New York, NY: Bantam Books, 1992.

Seliktar, Ofira. Politics, Paradigms, and Intelligence Failures: Why So Few Predicted the Collapse of the Soviet Union. Armonk, NY: M-E Sharpe Inc., 2004.

Shane, Scott. "Negroponte Confirmed as Director of National Intelligence," *New York Times*, 22 April 2005.

Shchien, Edgar H. "Groups and Intergroup Relationships." In *Classics of Organizational Behavior*. Edited by Walter E. Natemeyer. Oak Park, IL: Moore Publishing Company, Inc., 1978.

Simon, Hebert A. "Information 101: It's Not What you Know, It's How You Know It." *The Journal for Quality and Participation* (July/August 1998).

Skocpol, Theda. States and Social Revolutions: A Comparative Analysis of France, Russia, and China. Cambridge: University Press, 1979.

Smith, Bradley F. *The Shadow Warriors.* London: Andre' Deutsch, 1983.

Thibaut, J.W. and H.H. Kelley. *The Social Psychology of Groups.* New York: Wiley, 1961.

Thorne, C. Thomas, Jr., David S. Patterson, and Glen W. La Fantasie, eds. *Emergence of the Intelligence Establishment. Foreign Relations of the United States, 1945-1950*. Washington D.C., US Government Printing Office, 1996.

Troy, Thomas, F. "The Coordinator of Information and British Intelligence." *Studies in Intelligence*, 18, no. 1-s (Spring 1974). Previously declassified.

Troy, Thomas F. *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency*. Frederick, MD: Aletheia Books, 1981.

Troy, Thomas. "The Quaintness of the U.S. Intelligence Community: Its Origin, Theory, and Problems." In *Strategic Intelligence: Windows Into a Secret World (An Anthology).* Edited by Loch K. Johnson and James J. Wirtz. Los Angeles, CA: Roxbury Publishing, 2004.

Tuchman, Barbara Wertheim. *The Zimmerman Telegram.* New York: Viking Press, 1958.

US Code. Congressional Service. *Laws of the 80th Congress*, 1st sess. St Paul, MN: West Publishing Co., 1947.

US House. House Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations. *Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing, 24 August 2004*. Testimony of Bill Crowell, Markle Taskforce on National Security in the Information Age. On line. Internet 25 June 2005. Available from http://www.fas.org/sgp/ congress/ 2004/082404crowell.html.

US House. Permanent Select Committee on Intelligence. *IC21: Intelligence Community in the 21st Century*. Washington D.C.: US Government Printing Office, 1996.

US Intelligence Community. *US Intelligence Community Website*. On line. Internet, 15 January 2005. Available from http://www.intelligence.gov.

"U.S. Intelligence Failure Seen." *CNN News*, 13 May 1998. On line. Internet, 8 June 2005. Available from http://www.cnn.com/ WORLD/asiapcf/9805/13/india.cia.update/.

US Senate. Committee on Homeland Security and Government Affairs, "Lieberman Statement on Negroponte Confirmation," *Press Release*. On line. Internet, 5 July 2005. Available from http://www.senate.gov~gov_affairs/index.cfm?FuseAction=PressReleases. Detail&Affiliation=R&PressRelease_id=975&Month=4&Year=2005.

US Senate. Nomination of Robert M. Gates to be Director of the Central Intelligence Agency: Hearing of the Senate Intelligence Committee. 102nd Cong., 1991.

US Senate. Senate Select Committee on Intelligence. Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq. 108th Cong., 2004.

US Senate. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Final Report, Book VI: Supplementary Reports On Intelligence Activities.* Washington, D.C.: US Government Printing Office, 1976.

Waldrop, M. Mitchell. Complexity: The Emerging Science at the Edge of Order and Chaos. New York, NY: Touchstone, 1992.

Weber, Max. *The Theory of Social and Economic Organization.* Edited by Talcott Parsons. Translated by A.M. Henderson and Talcott Parsons. New York, NY: Oxford University Press, 1947.

Weiner, Tim. "Nuclear Anxiety: The Blunders; U.S. Blundered On Intelligence, Officials Admit." *New York Times*, 13 May 1998.

Wilson, Edward O. *Concilience: The Unity of Knowledge.* New York: Vintage, 1998.

Wilson, James Q. Bureaucracy: What Government Agencies Do and Why They Do It. New York: Basic Books, 1989.

Wines, Michael. "The Iraqi Invasion: U.S. Says Bush Was Surprised by the Iraqi Strike." *New York Times*, 5 August 1990.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision.* Stanford, CA: Stanford University Press, 1962.

Yergin, Daniel. Shattered Peace: The Origins of the Cold War and the National Security State. Boston, MA: Houghton Mifflin, 1977.

Zegart, Amy B. *Flawed by Design: The Evolution of the CIA, JCS, and NSC.* Stanford, CA: Stanford University Press, 1999.