A DESCRIPTIVE STUDY OF THE INTELLIGENCE COMMUNITY IN THE UNITED STATES OF AMERICA

Hursit Ucak, B.A.

Thesis Prepared for the Degree of

MASTER OF SCIENCE

UNIVERSITY OF NORTH TEXAS

May 2003

APPROVED:

Robert W. Taylor, Major Professor and Chair of
the Department of Criminal Justice
Tory J. Caeti, Committee Member
D. Kall Loper, Committee Member
David Hartman, Dean of the School of Community
Service
C. Neal Tate, Dean of the Robert B. Toulouse
School of Graduate Studies

Ucak, Hursit, A Descriptive Study of the Intelligence Community in the United States of America. Master of Science (Criminal Justice), May 2003, 109 pp., 2 illustrations, references, 83 titles.

This treatise represents a descriptive study of the intelligence community in the United States. It explores the ramifications of terrorism on the intelligence function, post September 11, 2001. In-depth discussions concerning the structure of the U.S. intelligence community are presented as well as a focus on the defined steps of the intelligence process: planning and directions, collection, analysis, production, and dissemination. The final aspect of this study poses questions and issues relating to the restructuring of the U.S. intelligence community in light of the Homeland Security Act of 2002.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

If we in intelligence were one day given three wishes, they would be to know everything, to be believed when we spoke, and in such a way to exercise an influence to the good in the matter of policy.

Sherman Kent

Since the early days of civilization intelligence has played an important role in many aspects of nations that it became a general saying “to be forewarned is to be forearmed.” It is impossible to determine when or how spying began, as there is no record of any ancient conflict in which spies were not used (Mahoney & Mahoney, 1998). Throughout history, kingdoms have been both created and overthrown by spies. Unpopular leaders have used spies to remain in power and saviors have led nations and peoples to new centuries through the work of spies. Therefore, it can be assumed that spying probably developed from a cave man’s first secret observation of a neighboring tribe. Of course, this was a modest beginning for a business that today uses very complicated electronic marvels (Mauer, Tunstall & Keagle, 1985; Mahoney & Mahoney, 1998).

The profession of intelligence has become more structured in recent years. There are more than forty American colleges and universities now offer courses in espionology (the study of intelligence) ranging from “Espionage in the Ancient World,” taught at the Georgetown University through “Espionage and History” at the University of New Hampshire, to Yale University’s “Intelligence and Covert Operations”(O’tole, 1988).

Furthermore, today there are several private organizations dedicated to the advance of espionology. The National Intelligence Study Center, The Consortium for The Study of Intelligence, and the Hale Foundation are only a few examples of this kind. All of these institutions encourage and sponsor the study of intelligence and the teaching of espionology in colleges and universities, and work to improve public understanding of the role of intelligence in national security. There are even some university programs that prepare people to go directly into a training program within an intelligence agency such as the CIA (Gannon, 2001; O'tole, 1988).

Traditionally intelligence communities have faced issues resulting from operating a large, complex organization effectively, the changes in technology, changes in society as a whole and changing political conditions.

September Eleventh Terrorist Attacks

With the September 11, 2001 terrorist attacks, a new era has started in both American and world history. U.S President, George W. Bush, called the attacks on the World Trade Center and Pentagon an act of war while others referred to them as attacks on civilization, democracy, liberty, and humanity. It is a war against invisible enemies all over the world including America that may last for years. In fact, terrorism is not a new problem, it is only now that the U.S. is feeling the direct effects of it. Terrorism, in many forms, has existed in foreign nations for decades. As it is the first time that the United States has faced this mysterious evil enemy, attentions have been focused on national intelligence.

While the sky was still filled with dust and smoke clouds rising from the World Trade Center and the Pentagon, doomsday scenarios and criticisms about the devastating terrorist attacks began to come from the national media: “A bigger (nuclear) attack on Manhattan!”,“Why didn’t the intelligence services forewarn?”, “The CIA was asleep at the switch!”, “The intelligence system isn’t working!”, “Reorganize top to bottom!”, “The biggest intelligence system in the world, spending up to $30 billion a year, could not prevent a group of fanatics from carrying out devastating terrorist attacks!”, “Drastic change must be overdue!” (Betts, 2002, p.2). Most of the criticism and questions raised in the aftermath of the attacks have centered on the question: What changes should the U.S. intelligence services make to be successful in fighting this war? At this point, experts are calling for reform and restructuring of all aspects of the intelligence field (Weiner, 2001; Calabresi, Ratnesar, McGirk & Ripley, 2002).

During the months that followed, the national nightmare about another calamitous terrorist strike went away as the U.S. struck back, the anthrax scare petered out and the fires at Ground Zero died down. The Bush Administration and Congress have mobilized massive amounts of government money, intelligence and personnel to track terrorists at home and abroad and tighten the country's protective net (Betts, 2002).

As the strategy of Al-Qaeda is to throw as many darts as possible at the board, it can be argued that a successful attack against the U.S. was an inevitability, no matter what precautions are taken. However, since the surprising attacks, the terrorists and other entities who are targeting the U.S. couldn’t be able to strike again. Therefore, it can be said that the U.S. intelligence and associated services have generally done well at protecting the country. (Betts, 2002; Calabresi et al., 2002).

In combating global terrorism, improving homeland security is also essential. Therefore, in October, the Administration created a new Office of Homeland Security to deal exclusively with the job of protecting the country from future terrorist threats. Billions of dollars have been spent so far toward reinforcing cockpit doors, tightening the airline baggage-screening process and hiring 28,000 new federal employees at airports to replace the private security firms that allowed al-Qaeda to slip through security precautions on Sept. 11 (Calabresi et al. 2002).

The controversial debate on fixing the U.S. intelligence agencies to better combat terrorism still continues. In order to better understand and assess the proposals that are made to improve U.S. intelligence capabilities, it is important to first examine the constraints the U.S. intelligence community has inherited.

Intelligence Constraints

The framework for U.S. intelligence was created in a different time to deal with different problems other than terrorism. The National Security Act of 1947, which established the Central Intelligence Agency (CIA), envisioned the enemy to be states such as the Soviet Union and also recognized the importance of protecting citizens' rights (Deutsch & Smith, 2002).

The result was organizations and authority based on distinctions of domestic versus foreign threats, law enforcement versus national security concerns, and peacetime versus wartime. The Federal Bureau of Investigation (FBI) is responsible for domestic intelligence, and the CIA, the National Security Agency (NSA), the Defense Intelligence Agency (DIA), and other agencies are responsible for foreign intelligence outside the U.S. Today, the U.S. intelligence community is composed of 13 advanced intelligence organizations dedicated to collect, analyze and disseminate intelligence and inform U.S. policy makers about ongoing events (Richelson, 1999).

Briefly speaking, law enforcement's focus is to collect evidence after a crime is committed in order to support prosecution in a court trial. The CIA collects and analyzes information regarding national security in order to forewarn the government before an act occurs. At this point, because of civil liberties, the FBI is reluctant to share information with other government agencies so as not to compromise future court action. Similarly, the CIA is reluctant to give information to the FBI for fear of its sources and methods of acquiring that information being revealed in court (Taylor, 1987; Deutsch & Smith, 2002).

According to Betts (2002), even the best intelligence systems can sometimes allow for mistakes to occur. Since counter-terrorism is a kind of competitive game these mistakes may result in destruction like that which occurred on September 11th Furthermore, terrorists are not inert objects; they are living and conniving strategists. Most frequently, terrorists fail and are caught before they strike, but because of the potential for error it is always possible that they may manage to get through and kill hundreds even thousands of people (Betts, 2002; Calabresi et al., 2002). America's national security system is designed to fight Soviets rather than suicide bombers (Calabresi et al., 2002). Therefore, reforms in intelligence process that can be undertaken now can make the intelligence community better. Making it much better, however, will ultimately require revising national norms such as educational norms and building new level of international intelligence cooperation (Betts, 2002).

It is also important to mention that even though reorganization seems like an appropriate response to failure, it should be the last way to improve performance during a critical situation. Because reorganization might create more gaps than it covers, and can increase the vulnerability of the country during the adaptation period. In addition, according to Betts (2002), the major underlying cause of mistakes in performance does not lie in the structure or process of intelligence agencies. But rather in the nature of the issues and targets with which intelligence has to cope; such as, well-trained opponents who strategize against it and alien cultures that are not transparent to American minds. Therefore coping with international terrorism has several dimensions and requires long-term strategic steps to be taken in order to be successful.

For now, making the U.S. intelligence community the scapegoat for September 11th catastrophe would only distract government agents and analysts from the critical task of identifying and preventing future attacks. Rather than going over the rumors of what intelligence did and did not do before September 11th it is more appropriate to focus on the possible immediate reforms in intelligence process and finding long-term strategic solutions to better combat global terrorism.

Research Purpose

From examining the dynamic nature of intelligence it is clear there are several controversial issues about intelligence that need to be studied, particularly in the aftermath of the September 11th terrorist attacks.

Improving U.S. intelligence to counter terrorism is a priority. Most scholars address the importance of data collection and intelligence analysis to be effective in combating terrorism. This has been considered a powerful tool in terrorism detection and prevention. Additionally, September 11th terrorist attacks showed some deficiencies in intelligence dissemination and coordination between local and federal agencies. To this regard, some scholars argue that more federal efforts are needed to improve dissemination of intelligence between agencies and with state and local authorities. In addition an intelligence fusion center is needed at federal level to collect, analyze, and disseminate intelligence on a need to know basis. These and other related issues are considered important in combating terrorism and discussed in this study.

Another important aspect of combating terrorism is protecting the country from future attacks. Since September 11th the Administration and Congress have taken several steps to improve homeland security which include a proposal to create a Cabinet-level Department of Homeland Security (DHS), increasing security at the borders, enhancing the nation's stockpile of smallpox vaccine, and enhancing cooperation and communication with state and local governments and civic institutions. These and some other important applications of the government are also studied in this research. Moreover, some important recommendations of the scholars regarding to homeland security are discussed. These include expanding the training programs for first responders during chemical biological radiological and nuclear attacks, establishing a national health surveillance network that could detect the presence of a bio-terrorist attack at early stages and defining the role of National Guard, which is well-positioned to assume the lead military role in homeland security.

To understand these and other issues studied in this research first, the purpose and function of intelligence is examined, the structure of U.S. intelligence and its elements are explored and the types of intelligence that they collect are discussed. Later, the intelligence process in regard to the intelligence cycle is explained. Since intelligence analysis has become the most important part of intelligence process as a result of sophistication in technology it is discussed in detail in regard to the factors of evaluation in intelligence analysis. Finally, dissemination of intelligence is examined by analyzing the outputs of the U.S. intelligence community.

After understanding the purpose, structure and process of intelligence selected issues about U.S. intelligence community and homeland security are discussed in detail. Indeed, these two areas of focus are expected to support the policy makers.

Limitations

There is considerable difficulty in framing of the research on intelligence because of the complexities of issues related to the subject. For this reason, it is important to make it clear what is and is not included in this study. To begin with, even though it is not possible to exclude completely, terrorism and organized crime will not be the studied in dept. Intelligence plays a vital role in combating both terrorism and organized crime and it would be impossible to fight terrorism or organized crime without support of intelligence, especially in terms of national security, drugs, weapons and nuclear materials trafficking. However, for the purpose of this study, terrorism and organized crime will be recognized as specialized areas to be studied separately.

Second, the issues discussed in this study do not represent the problems of the intelligence services other than that of the United States. This research will only examine the U.S. intelligence community because of the significant effects of September 11th events. Since U.S. intelligence is considered the leading and most advanced intelligence organization in the world because of the advanced technology it uses, finding solutions to its problems will directly or indirectly solve many of the problems of other countries' intelligence services as well.

The structure of the U.S. intelligence community will be touched upon in the second section, but it will be limited to the research related to intelligence analysis. In the same chapter there will be a discussion on the intelligence cycle associated with strategic intelligence, similar limitations will apply to this topic.

Another limitation of this study is confidentiality. Because of the secret nature of intelligence, intelligence agencies do not give information to researchers and deny applications for research. Therefore, detailed information about the applications of intelligence departments especially about intelligence analysis is not available. For instance, there is little information about the computer software that is used in the analysis of intelligence. Without having illustrative cases in which intelligence analysis techniques were used, it is impossible to measure the effectiveness of the methods of intelligence analysis.

All of the information presented in this study is derived from openly available sources. It is important to note that secrecy has an important effect on the openly available sources on the subject. Most of the books and articles in the field are written by retired senior professionals who have vowed not to communicate certain types of information without authorization and are bound by the special restrictions of the current Official Secrets Act. For the protection of current and future sources there is an official scrutiny procedure. As a result of this, their books or articles are subject to certain deletions and changes. Once security clearance is given they are allowed to be published.

As mentioned above, this research only considers open sources that are widely available. It will not delve into the secret, human, or technical means of collecting information. Therefore, in this study all of the critiques, problems and solutions are obtained by comparing and contrasting the points stressed in different books and articles, most of which were written by current or retired senior professionals that have extensive knowledge and expertise in the field.

In sum, there is a limitation in data acquisition about the issues discussed in this research because of the secret nature of intelligence. In addition to the limitations mentioned above, there are other limitations:

- Reliability of the information which is based on intelligence sources. We should always remember the possibility that the information might be disseminated as a part of on going disinformation operation.
- Personal interpretations. One of the major sources of information is dairies, experiences of ex-agents.
- Timeliness of and public interest on the subject. After the September 11th terrorist attacks public attention has been placed on terrorism and intelligence which led researchers and general public to read and search the sources that are available openly. Therefore, many of the resources are not available in libraries. This unexpected public interest caused lines especially on books that were available at the libraries.

This study will define intelligence and its purpose, examine the intelligence process and its outputs, explore structure of U.S. intelligence, intelligence analysis and dissemination of intelligence, and discuss some selected issues about intelligence and homeland security and conclude with some ideas for further consideration.

Methodology

The method used in this study is a comprehensive literature review. Before starting the methodology, it is important to mention that the researcher has worked for the

Intelligence Department of the Turkish National Police for seven years. During that period of time he took part in several anti-terrorism intelligence operations as a case officer both in Europe and the Middle East.

Since this study is a comprehensive literature review much of the research is library-based, along with some dependable resources from the Internet.

The present study has three steps. The first step is the preparation for the study. The second step is data collection about intelligence analysis and strategic intelligence issues. At this step, information about the structure and intelligence process of U.S. intelligence is also gathered to understand the nature of problem. The third step is to analyze and conceptualize the gathered data.

In this context, this study started with a literature review including academic sources from books, journals, reports, and intelligence related Web sites designed by both governmental and non-governmental organizations to outline the state of knowledge and argument in the field.

After exploring the relevant historical, legal and structural information the data was synthesized to determine necessary improvements in intelligence analysis and strategic intelligence capabilities of U.S. intelligence for effective detection and prevention of terrorism. In doing so, the researcher took caution to avoid biases, personal interpretations, rumors and psychological operation based information that can be associated with the intelligence field to overcome some research-based problems such as reliability.

Overview of Forthcoming Chapters

This study is comprised of five chapters including the first chapter.

In Chapter 2, intelligence and related terms are defined. In addition, structure and intelligence process of the U. S. intelligence community are explored. To explain the intelligence process in the U.S., the intelligence cycle is examined.

Chapter 3 is devoted to intelligence analysis, the most important part of the intelligence cycle, and dissemination of intelligence in the U.S. Additionally, factors of evaluation and products of intelligence are also discussed to better understand the intelligence process.

In Chapter 4, since homeland security and intelligence have become the priority of the government in the aftermath of September 11th terrorist attacks, selected issues about the acts of government are analyzed and further recommendations of the scholars to improve these two major areas are discussed in detail.

Chapter 5 is a conclusion and contains recommendations for future improvement.

CHAPTER 2

DEFINITION AND PURPOSE OF INTELLIGENCE

The Department of Defense dictionary (2002) defines intelligence as information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

The Oxford English dictionary offers examples of the use of the word intelligence in the sense of "communications of spies, secret or private agents, etc." as early as the sixteenth century, and instances in which it has been used to mean "the agency for obtaining secret information; the staff of persons so employed, secret service."

According to *Air Force Intelligence and Security Doctrine* (1996), intelligence is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.

In the *Rockefeller Commission Report to the President* (1975), intelligence is defined as information gathered for policymakers which illuminates the range of choices available to them and enables them to exercise judgment. Good intelligence will not necessarily lead to wise policy choices. But without sound intelligence, national policy decisions and actions cannot effectively respond to actual conditions and reflect the best national interests or adequately protect national security.

Godson (1992) contends that intelligence can be defined within two broader concepts. The first holds that intelligence is information relevant to the national security of the state such as the territorial sovereignty and safety of its inhabitants. The alternative concept embodies intelligence as that information which is sought by the state with regard to the secrets, capabilities and intentions of its adversaries.

Timely, accurate, and relevant intelligence provides mission focus, reduces the risk of surprise, and enhances operational effectiveness (Air Force Intelligence and Security Doctrine, 1996).

McCarthy (1998) defines intelligence as information, which has been identified as relevant, collected, verified, interpreted within the context of specific objectives, analyzed, classified and distributed to the policymaker who utilizes it towards the persistence and prosperity of the state.

Intelligence gathering takes place for both tactical and strategic purposes.

Tactical intelligence is primarily the responsibility of agencies within the military services. Tactical intelligence provides advantages on the battlefield against hostile military forces or terrorist groups through direct support to operational commanders in areas such as reconnaissance, mapping, and advanced warning of enemy movement (Richelson, 1999).

According to Ransom (1973), the meaning of strategic intelligence is evaluated and processed information about the power and intentions of foreign nations or other external phenomena of significance in decision-making council. Generally the term refers to the informational needs of national government officials, particularly foreign and defense policy makers (Berkowitz & Goodman, 1989).

In the Oxford English dictionary the term strategy implies the economic allocation of resources toward the attainment of objectives. The importance of this definition is that it incorporates evaluated information (intelligence) as an essential and unavoidable element in any conception of a decision-making system.

The common meaning of strategic intelligence is the evaluated information needed at the highest policy-making levels for the economic allocation of resources not only toward national objectives, but also toward the formulation of such objectives (Richelson, 1999).

Intelligence for strategic purposes (national intelligence) serves foreign policy, national security, and national economic objectives. National intelligence focuses on foreign political and economic events and trends; strategic military concerns such as plans, doctrines, scientific and technical resources; weapons system capabilities; and nuclear program development (Richelson, 1999).

According to Kent (1969), there are three major functional strategic intelligence categories: (1) basic descriptive or generalized information usually pertaining to “hard” or “knowable” data, such as population or economic facts; (2) current reportorial or current estimate information, such as the political party alignment in a foreign nation at a given instant; and (3) speculative-evaluative, or the forecasting or warning kind of information, such as a prediction that a particular government will fail a vote of confidence in its parliament next week.

According to Kendall (1949), the key role of strategic intelligence is not to identify specific operational targets. It is to focus attention on new threats, to identify changing situations and to provide the basis for forecasting future trends.

It is important to mention here that even though there is distinction between strategic and tactical intelligence, it is vanishing under the impact of fast communications and accelerating technology (McCarthy, 1998).

Kent versus Kendall debate

There are two fundamental approaches to intelligence: the traditionalist and the activist approaches. The traditionalist approach is based upon the intelligence doctrine of Sherman Kent. This view contends that there should be a definite boundary between the domain of the intelligence producer and consumer, the policymaker.

Traditionalists argue that it is not the place of the intelligence producer to become actively involved in policy decisions, and that policymakers and intelligence producers must keep their distance, or “suffer the wrath of subjectivity” (Heymann, 1985, p. 58). The traditionalists view the policy process as a prescribed sequence of events into which the intelligence community feeds sterile facts arrived at through deductive analysis of surreptitiously obtained secrets while having no part in the application of those facts to the objectives (Hilsman, 1956; Hulnick, 1986).

The activist philosophy is based on the principle of intelligence performing more than just a timely presentation of the facts to the consumer (Brammer & Hulnick, 1984). The purpose of the intelligence function in this context is to play an active role in influencing the decision making process by presenting the decision maker with facts which in a timely manner can enable the consumer to seize the initiative (Kendall, 1949; Davis, 1992).

This approach implies a relationship between intelligence and policy, with intelligence producers more actively disposed towards policy objectives and action based upon perceived opportunities (Laurer, 1985).

While Kent and Kendall differ over the nature of the relationship between intelligence analysts and policymakers, their doctrines have a fundamental point in common. This point of convergence is on the importance of getting the relationship between analysts and decision makers right. Both realize the importance of communication and interaction between producers and consumers.

Taylor (1987) adds a third school to the Kent – Kendall debate. A new version of the second school that is a result of sophistication in technology, whose main concern is predicting future events not only to avoid policy drawbacks and political mistakes by giving accurate information, but also to plan course of action for achieving specific goals and objectives. The improvement in computer technology especially in data storage and intelligence analysis software systems has made the prediction of future events possible for analysts.

Structure of the U.S. Intelligence community

The U.S. collects data via reconnaissance satellites, aircrafts, ships, signals intercept, seismic ground stations, radar, undersea surveillance, and traditional overt and clandestine human sources. It processes and analyzes the data collected, using the most advanced computers and a variety of specially developed techniques for extracting a maximum of information from the data. The total cost of these activities is approximately $27 billion per year (Weiner, 1998). Given the wide range of activities and the large number of intelligence consumers, it should not be surprising that a plethora of organizations are involved in intelligence activities.

Traditionally the U.S. intelligence community is composed of 13 main organizations, which are defined in a number of government publications, directives and regulations. These are: the Central Intelligence Agency, the National Security Agency, the National Reconnaissance Office, the National Imagery and Mapping Agency, the

Defense Intelligence Agency, the Bureau of Intelligence Research of the State Department, the intelligence elements of Military Services, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the intelligence components of the Department of Energy and the Department of the Treasury. In addition to these, the Unified Commands and the Department of Commerce have also their own intelligence elements (Johnson, 1996).

According to Richelson (1999), the continued major role of U.S. service intelligence organizations is partly a function of bureaucratic politics, partly a function of law, and partly the result of the structure and the requirements of the U.S. military.

Richelson (1999) groups the intelligence elements of the U.S. intelligence community into five categories:

-National intelligence organizations

-Department of Defense intelligence organizations

-Military service intelligence organizations

-The intelligence components of Unified Commands

-Civilian intelligence organizations.

National Intelligence Organizations

According to Richelson (1999), four of the intelligence organizations mentioned above are considered to be national level intelligence organizations: The Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Imagery and Mapping Agency (NIMA).

These organizations perform intelligence functions on behalf of the entire government rather than just a department or military service. Their actions provide intelligence for national –level policymakers, and they are responsive to direction by supra-departmental authority (Johnson, 1996).

Department of Defense Intelligence Organizations

In addition to the national intelligence organizations under the Department of Defense, the department has its own agency, the Defense Intelligence Agency (DIA). The DIA operates in support of the Secretary of Defense, the Joint Chiefs of Staff, and military commanders (Richelson, 1999).

The DIA contains within it a service for collection of human intelligence in addition to two intelligence production centers that had previously been operated by the Army, one focused on space and missile systems and the other on medical intelligence.

Military Service Intelligence Organizations

According to Johnson (1996), a military force with large service components and major combat commands distributed across the globe may be better served in terms of intelligence support by organizations that are not too detached from the service components and the command.

Army Intelligence Organizations

U.S. Army intelligence collection and production activities are the responsibility of the Deputy Chief of Staff for Intelligence (DCSI) (Herman, 1996). Those operations are carried out by the U.S. Army Intelligence and Security Command (INSCOM), and the National Ground Intelligence Center (NGIC). INSCOM conducts imagery, and signals intelligence (SIGINT) operations, and NGIC produce scientific and technical, in addition to general military intelligence (Richelson, 1999).

The DCSI determines Army intelligence policy, and supervises the activities of INSCOM and NGIC. It also represents the army in military and national intelligence arenas (Johnson, 1996).

Navy Intelligence Organizations

The Office of Naval Intelligence (ONI) represents the head of the naval intelligence community and is responsible for management and direction of naval intelligence activities. It consists of four departments: Technical Operations, Collection Management and Requirements, International Programs, and Specific Programs (Richelson, 1999).

Air Force Intelligence Organizations

Two Air Force organizations perform departmental intelligence activities: the Directorate of Intelligence, Surveillance, and Reconnaissance (DISR) and the Air Intelligence Agency (AIA). The Air Force Technical Applications Center (AFTAC) is the head of Air Force intelligence and serves the entire Air Force intelligence community (Richelson, 1999).

Unified Command Intelligence Organizations

The Unified Commands consist of forces drawn from all the military services. There are five unified commands focusing on specific regions of the world: the Atlantic Command (USACOM), Central Command (USCENTCOM), European Command (USEUCOM), Pacific Command (USPACOM), and Southern Command (USSOUTHCOM). In addition to these there are four additional commands that have worldwide responsibilities: U.S. Space Command, U.S. Special Operations Command, U.S. Strategic Command, and U.S. Transportation Command (Richelson, 1999).

The role of the unified commands from the point of intelligence is supervision of national reconnaissance and other sensitive collection operations conducted within their territory and intelligence analysis for both the command and higher authorities (Richelson, 1999).

Civilian intelligence organizations

Offices in the departments of State, Energy, Treasury, Commerce, Justice and Transportation conducts intelligence activities on foreign political and military affairs, and narcotics trafficking. All of these agencies make contributions to the national intelligence effort in addition to their primary responsibility to their department (Johnson, 1996). These agencies include:

-Department of State: Bureau of Intelligence and Research (INR).

-Department of Energy: Office of Energy Intelligence (OEI).

-Department of Treasury: Office of Intelligence Support (OIS).

-Department of Commerce: Office of Executive Support (OES), Office of Export Enforcement (OEE).

-Department of Justice: Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA).

-Department of Transportation: Office of Intelligence and Security.

Types of Intelligence In The U.S. Intelligence Community

Political Intelligence

Political intelligence includes both foreign and domestic politics. It is obvious that foreign policies of other nations have an impact on the United States (Richelson, 1999). For instance a nation’s support or opposition to NATO, a country’s political and economic relations with terrorist-sponsoring countries (e.g. Iraq or Afghanistan), or their attitudes and policies concerning vital areas such as the Middle East, directly or indirectly affect the interests of the United States.

Domestic politics of other countries, whether friendly, neutral or hostile, are also significant concerns of the U.S. According to the National Intelligence Council (1997), most conflicts in the world are internal and not between the nations. Therefore the presence or resolution of such conflicts can have an effect on the regional power balance, on the presence of U.S. military bases in a region, or on the accessibility of critical resources (like oil) to the U.S. (Richelson, 1999).

Military Intelligence

The U.S. should always be aware of the capabilities of potential adversaries in order to determine its own military requirements whether nuclear, conventional or special operations. Additionally, military intelligence is essential to assess the balance of power between the pair of nations whose conflict can affect the U.S. interests. Moreover, military intelligence is required to assess the need and impact of any military aid that the U.S. may be asked to provide (Treverton, 2001). Furthermore, military intelligence is required for the protection and security of U.S. military bases and troops located overseas.

Scientific and Technical Intelligence

Civilian and military related scientific and technical developments are another area of concern for the intelligence community. Most of the technological developments that occur in the civilian sector have military applications too. For instance computer technology, biotechnology, mirrors and optical systems, and lasers can also be used for military purposes. Countries who focus their technology on these fields or absorb foreign produced technology in those areas mostly use it for military purposes. Therefore, these nations receive special attention of the U.S. intelligence (Laquer, 1985).

Another aspect of scientific and technical intelligence is atomic energy intelligence. Whether the announced purpose of a country’s atomic energy activities has been civilian or military, those activities have a high intelligence priority for the U.S. intelligence community (Richelson, 1999).

Economic Intelligence

Knowing the strengths and vulnerabilities of nations economy is always essential to understand and assess their capacity for conflict. Another point of interest in economic intelligence is the availability and pricing of key resources for the U.S. economy such as oil. It also concerns topics such as sanction busting, money laundering, terrorist financing, bribery and corruption, and economic espionage (U.S. Congress Senate Select Committee on Intelligence, 1997).

Sociological Intelligence

Sociological intelligence examines group relations within a particular nation. The relations between the ethnic, religious or political groups can have a significant impact on a nation’s stability as well as on the nature of its foreign policy (Hastedt, 1991).

The Intelligence Process

Intelligence Cycle

Intelligence production is generally presented in the literature as a sequential process and is explained in terms of an intelligence cycle. Historically, the process of intelligence production has been cyclical. A basic understanding of the intelligence cycle is necessary for both intelligence practitioners and consumers. Intelligence cycle is the steps by which information is converted into intelligence and made available to the user. These steps represent sequential phases of planning and direction, collection, processing and production, analysis and dissemination (Godfrey & Harris, 1971). Schneider (1994) explains this process in nine interrelated stages: planning, collection of information, assessment of information validity, collation of information, analysis of information, assessment of analytical rigor and value, dissemination of intelligence, application of intelligence, and the review and assessment of the criminal intelligence function or unit. Most experts agree with Godfrey and Harris and explain the intelligence cycle in the above five stages. However, these steps should not be viewed as separate elements but as an interrelated whole.

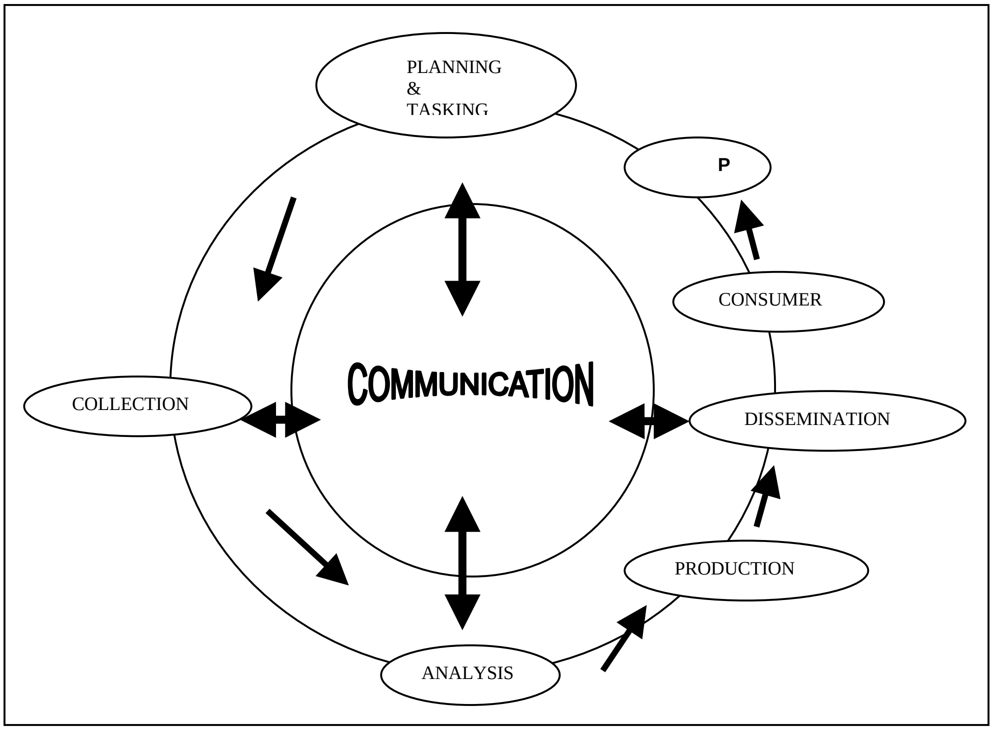
Planning, which entails the prioritization of information demands and the allocation of resources, represents both the first and the last stage. Information is collected from a variety of sources, processed into useful form, analyzed, by drawing upon all available sources to generate balanced conclusions, and disseminated to the consumers of intelligence.

Consumers of intelligence include the President, analysts, national security officials, and others in the executive and legislative branches of government with a need for information to support national security decisions. Dissemination of finished intelligence products may stimulate demand for new requests for intelligence information (McCarthy, 1998).

Whereas the steps of intelligence cycle as described usually follow one another in sequence, the function of communication is ubiquitous and takes place continuously throughout the process. Communication is the lubricant of the cycle (McCarthy, 1998). Communication not only enables interaction between the separate components of the intelligence system, but it also provides an essential link between the intelligence community and its external environment. It conveys intelligence requirements from the consumer to the intelligence community. After the production process the intelligence products are disseminated to the consumer. Communication also provides the decision maker with information on the impact of their policy initiatives on the external environment (McCarthy, 1998).

Without communication throughout the entire process no cyclical connection could exist, “goals would be ill defined, thread perception would be difficult to conduct and responsive adaptation to the dynamics of the environment would be dysfunctional” (McCarthy, 1998, p. 55). Communication can therefore be described as the axle upon which the intelligence cycle rotates. See figure 1.

Figure1: Intelligence Cycle



Source: [McCarthy, 1998, p. 43].

Planning and Direction

In the context of the intelligence cycle, planning entails the identification of collection priorities in response to requests from intelligence consumers. The planning and direction process involves the management of the entire intelligence effort, from the identification of the need for data to the final delivery of an intelligence product to a consumer (Godfrey and Harris, 1971). The process may be initiated by requests or requirements for intelligence based on the needs of the President, the departments of the State, Defense and Treasury or other consumers. In some cases the requests and requirements become institutionalized. For instance, the intelligence community need not be reminded to collect information on nuclear proliferation in China, this intelligence requirement is understood without a formal request. An example of the planning stage is the determination of how many surveillance satellites the United States needs, the corresponding allocation of financial resources made available by Congress, and the continual process of selecting targets at which the satellites' cameras and antennas should be aimed (Richelson, 1999).

According to Schneider (1994), there are four interrelated ways of planning in the intelligence cycle: conducting an environmental scan, choosing a topic for inquiry, defining the problem, and developing a collection plan. Planning of collection efforts is an essential element of the intelligence cycle because the United States has a limited amount of intelligence collection assets. A central authority is needed to weigh competing demands for collection and decide which collection assets should be assigned to which tasks. Far more requests for collection are submitted by various users than are actually approved (Martens, 1990).

According to Richelson (1999), national intelligence planning, management, prioritization, and resource allocation are overseen by the Directory of Central Intelligence (DCI), as well as the Deputy Director of Central Intelligence. The DCI chairs the National Foreign Intelligence Board, which includes officials from the DoD, NSA, FBI, and other agencies and advises the DCI on both analytical and administrative issues. The National Intelligence Council, comprised of senior intelligence experts inside and outside the government, produces National Intelligence Estimates, assess the quality of analyses, and identify critical gaps that require new collection priorities.

Collection

Collection involves the gathering, by a variety of means, of raw data from which finished intelligence will be produced (Hicks, 1998). Collection of foreign intelligence relies heavily on technical means. The bulk of the intelligence budget is for acquisition and operation of technical systems, most of which are related to collection (Nelson 1993). Technical collection assets include various satellites; ground-based monitoring stations; and airborne, ocean surface, and underwater platforms (Godfrey & Harris, 1971).

Technical collection methods are categorized broadly as image intelligence (IMINT) and signals intelligence (SIGINT). IMINT is collected from aircrafts, and satellites (Nelson 1993).

According to Nelson (1993), SIGINT is the monitoring of electronic signals. These include intercepted radio, microwave, satellite, and telephone communications; telemetry, such as data streams transmitted during ballistic missile tests; and radar emissions. Some signals are intercepted through the antenna arrays of ground stations around the world, which monitor broadcast, satellite-linked, and other radio communications. Space-based SIGINT collection comes from a variety of satellites. The NSA is the lead agency for SIGINT.

Historically, technical collection means have been critical in the verification of arms control agreements, through monitoring of missile tests, radiation and seismic detection, and direct observation of nuclear production facilities and weapons sites (Adarn, Zorpette, Meyer & Horgan, 1986).

Nontechnical intelligence collection can be open or covert. Although there is substantial debate over the extent to which the intelligence community (particularly the CIA) has made effective use of open-source intelligence, it is widely recognized that a great deal of relevant information about foreign political, economic, military, and other issues is publicly available (Steele, 1993). Other potential open sources of material for intelligence analysis include foreign broadcasts and newspapers; academic, scientific, and trade journals; books; scientific conference reports; diplomatic contacts (e.g., foreign attaches); and debriefings of U.S. scientists and business people who attend international meetings (Godson, 1989).

Clandestine nontechnical intelligence collection is the concern of human intelligence, or HUMINT. Case officers, usually operating under cover as U.S. officials in foreign posts, are the backbone of this effort. Through their political, economic, and social contacts, case officers recruit local agents to provide information unavailable through technical means. Placement of agents under nonofficial "deep" cover may facilitate entry into particularly difficult to penetrate organizations such as drug cartels; however, deep cover involves potentially greater risk to the agent (Godson, 1989).

Processing and Production

Processing is concerned with the conversion of the vast amount of information coming into the system to a form suitable for the production of finished intelligence. It involves interpretation and measurement of images and signals, language translation, decryption, sorting by subject matter, and data reduction (Schneider, 1994).

Godfrey and Harris (1971), argue that the purpose of processing is to determine the reliability and validity of the raw information. Therefore, when information is gathered, it is evaluated within the context of the purposes previously decided in planning stage (Schneider, 1994).

The information collected by intelligence assets, especially technical means, must be converted to a usable form before it can be analyzed. Encrypted communications have to be decrypted for maximum utility (although full decryption may not be necessary for traffic analysis, which itself provides some useful information); language experts translate SIGINT into English; IMINT is processed electronically to assist in interpretation of imagery (Richelson, 1999).

Analysis

The analysis and production process entails the conversion of basic information into finished intelligence. It includes the integration, evaluation, and analysis of all available data and the preparation of various intelligence products (Godfrey & Harris, 1971). Because the raw intelligence that is collected is often fragmentary and at times contradictory, specialists are needed to give it meaning and significance. According to Taylor (1987), intelligence analysis is the heart of the intelligence cycle.

According to Berkowitz and Goodman (1989), all-source analysis is the basis of the intelligence production effort. All-source analysis converts collected information from multiple sources into finished intelligence products that are useful to intelligence consumers. Extensive editing and prioritizing are necessary to reduce and simplify the voluminous stream of collected data.

According to Peterson (1998), the practice of analysis, involves more than editing. In the traditional view of the intelligence community, all-source analysis is both science and art. It includes integration and evaluation of all available data, finding patterns among fragmentary or contradictory sources, and drawing inferences from incomplete evidence. Whereas all-source analysis can add significant value to raw information, it is subject to potential pitfalls that can lead to major errors. These include, for example, a lack of awareness of other cultures leading to "mirror imaging"--the assumption that foreign policy makers will behave as Americans would. Over reliance on clandestine or technical sources, simply because they are uniquely available to intelligence analysts, is another risk (Berkowitz and Goodman, 1989).

Harris (1976) mentions analysis as the key element for success in an intelligence operation. Analysts, who are typically regional or subject matter specialists, prepare a variety of products for intelligence consumers. These include: current intelligence on political and other events; encyclopedic intelligence, which is compilations of data for future use, such as maps or economic statistics; and estimative intelligence, which is predictions of trends and events, with a focus on potential threats to U.S. security.

The traditional view of analysis, developed in the CIA's early history and incorporated into its training for many years, held that analysis should be conducted at arm's length from intelligence consumers. This distance would enable analysts to avoid being biased by domestic political concerns (Godson, 1989).

More recently, a competing view has emerged within the intelligence community that analysts should actively seek to meet the specific needs of policy makers, for example, by identifying opportunities for proactive measures of intelligence collection that advance U.S. policies.

Dissemination

The final step of the cycle is dissemination of the finished product to consumers. It involves the distribution of the finished intelligence to the consumers; the policymakers and operators whose need triggered the intelligence process.

Schneider (1994) recommends that before disseminating the product to the consumers, managers should control the intelligence product in terms of the accuracy of the intelligence, logical flow, and rigor not to mislead the consumer.

Finished intelligence prepared under the DCI's direction is hand carried daily to the President and key national security advisers. Other selected intelligence products, such as classified papers and encrypted electronic documents, are distributed to national security planners and policy makers on the basis of their need to know, as determined, in most cases, by the intelligence community. Broader, longer-range products prepared under the National Intelligence Council's direction are disseminated as National Intelligence Estimates (Richelson, 1999).

As these dissemination efforts lead to new requirements for information, the intelligence cycle begins again.

CHAPTER 3

INTELLIGENCE ANALYSIS AND PRODUCTION

To the layperson, intelligence might seem like secret documents produced by government agencies to run covert operations and overthrow unfair regimes. Intelligence, however, is primarily a process of collecting raw data, filtering, analyzing, and finally coming up with some logical conclusions. Analysis is the step in which raw data is processed and converted into meaningful information (Godfrey & Harris, 1971).

Intelligence analysis is the art of telling a story about the past, present and possible future of a subject. The end of the process is delivering this "intelligence" product to someone who can act on it. The action can do nothing more than a confirm a decision-maker's activity or motivate the decision-maker to modify their current actions.

Gottlieb, Arenberg, and Singh (1994), define intelligence analysis as the systematic collection, evaluation, analysis, integration, and dissemination of information on targets, especially related to their associations and their identification with criminal activity. The analysis step in the intelligence cycle is considered the most important. Schneider (1994) states that policy makers, administrators, and prosecutors should use the product, which is a result of analysis in the intelligence cycle, to create new and more effective policies. According to Harris (1976), analysis is the key element for the success of intelligence units.

The Purpose of Intelligence Analysis

As mentioned in the second chapter, Taylor (1987) proposes three fundamental approaches concerning the purpose of intelligence analysis. First, the traditional approach, which is based upon the intelligence doctrine of Sherman Kent. This view contends that there should be a definite boundary between intelligence producer and consumer. In other words the analysts should provide statistical support on past events and leave the policy to policymakers. According to this view there are no follow up investigations regarding to the policies.

The second one is the activist philosophy. The remit of the intelligence function in this context is to play an active role in influencing the decision making process by presenting the decision maker with facts which in a timely manner can enable the consumer to seize the initiative (Kendall, 1949; Davis, 1992). This approach implies a relationship between intelligence and policy, with intelligence producers more actively disposed towards policy objectives and action based upon perceived opportunities (Laurer, 1985).

The third school is a new version of the activist school as a result of sophistication in technology, whose main concern is predicting future events not only to avoid policy drawbacks and political mistakes by giving accurate information, but also to plan a course of action for achieving specific goals and objectives (Taylor, 1987).

Evaluation for Intelligence Analysis

More information is now available to the analyst than ever before as a result of the information revolution. For instance, the NSA can collect the equivalent of the entire collection of the Library of Congress in three hours (Cahlink, 2001). However, more information is not necessarily synonymous with better information. To intelligence consumers, the product is only as credible as the sources from which it comes. And this basic concept that intelligence must be based on credible objective information is the exact reason why it is important to evaluate sources for intelligence analysis (Cahlink, 2001).

In order to develop reasonable and objective intelligence, one must begin with sources that provide simple truthful facts. Since an analyst must look at all aspects of an event or situation, sources are sought which are authoritative, provide varied perspectives, and are perceptive. Sources from which intelligence is produced must also be timely and easy to use.

Factors of Evaluation in Intelligence Analysis

According to Center for Media and Public Affairs [CMPA] (2002), there is little difference between evaluating methods developed by library scientists and those of intelligence agencies. Both reflect on a source's accuracy, timeliness, accessibility, and content. However, intelligence agencies pay particular attention to a source's bias, veracity, and timeliness in order to evaluate it for analysis. Other factors to consider include a source's uniqueness, credibility, scope, depth, tip factor, and other costs of getting useful information for intelligence (Foreign Broadcast Information Service [FBIS], 2002; International Press Institute [IPI], 2002).

Uniqueness

Sources range from primary to secondary. Uniqueness is similar to authority that considers the concept of in-house experts investigating stories rather than using other agencies to provide them news (FBIS, 2002). If a source is primary, then analysts should answer the following questions: Are authors cited? Do these authors explain how they come across their information? Are citations complete?

In the case of a source citing another source, it should be remembered that these may actually be feeds from newswires, written and rewritten as original stories. Rewrites often take on their own ideas, and their own conclusions. In the case of secondary sources, it is more sensible to refer back to the original source to ensure that the accuracy of the information is retained (IPI, 2002).

Biases

Sources can be based on facts or deliver a particular message. Webster dictionary defines bias as a “predisposed point of view”. Bias can come in all shapes and sizes. There is geopolitical bias or religious bias for instance. Culture plays a large role in the way an event is covered as well. What may be considered acceptable in one culture may not be acceptable in another. In addition, economic bias is evident if only one aspect of statistics is covered, but others are omitted (IPI, 2002).

The ownership of a publication also has an effect on the type of information and its meaning. If the source is owned by the state from which the publisher resides, then it may be influenced by that state's values. Therefore, learning about where the source comes from, where it is published, who pays for its existence, and who owns it is always crucial in intelligence analysis (CMPA, 2002).

Credibility

Sources should be believable and have a stainless reputation otherwise they become questionable and difficult to believe. To evaluate sources the following questions should be asked by the analysts: Are the sources believable? Do they seem to be well informed about the topics they are reporting? Do they offer insights? Do they tell the whole story? Are they known to be authoritative, or are they considered sensationalistic journalists? (FBIS, 2002).

Veracity

Sources break stories or report facts from other news agencies. At this point analysts should answer the following questions to evaluate the veracity of the sources: Is the information provided easily verifiable by another source? Is the information well cited? Is there a bibliography? Are the sources used authoritative?

Discerning the veracity of an intelligence source is of the greatest importance because if a source cannot be verified, it cannot be considered factual or credible (CMPA, 2002).

Scope

Sources can either spread their coverage over a variety of subjects or focus on specific areas. Since the objective of intelligence analysis is to provide a complete picture of an issue, all aspects of it must be examined. Part of the collection process is to identify relevant information from disparate sources; it is always favorable to have several sources that provide complete coverage of an event or issue (FBIS, 2002).

Tip Factor

During the collection process, sources range from straight factual accounts to providing analytical clues of a situation for further investigation. This is important for intelligence because analysis is about understanding the breadth as well as the depth of an event or situation. Sources should help the analyst to put together all the facts of the story or point to sources that complete the story (IPI, 2002).

Depth

Sources run the range of general descriptions and in-depth analysis. Related to scope is the depth at which a source will cover an issue. Does the source only provide a general description of an event? Or are details given such as persons, places, names, times, significance, background, technical aspects, etc.? (CMPA, 2002). These questions are essential because details provide a better understanding of a situation or a system's capability. It may reveal system capabilities, problems not considered before, and a better understanding of what can be done about them.

Timeliness

Sources range from current to historical coverage. For the most part, intelligence analysis requires current sources for its products. For this reason, a majority of open-source intelligence information comes from news sources.

However, historical documents that will give insight into the topic that is being covered should not be discounted. Analysts have to remember that intelligence analysis is telling a story of the past, present, and possible future of a situation or topic which means that historical as well as current sources must be referenced (CMPA, 2002).

Costs

Sources lie on a spectrum from the ones that are very easy to assimilate to those that take extensive work to utilize. Most of the sources are difficult to identify. For instance, they may be in a format or a language that is difficult to use, or they may be in a country that cannot have export restrictions placed upon them. In addition, the source may be too technical to be useful, it may not be written clearly, or may be difficult to navigate (FBIS, 2002; IPI, 2002).

Misinformation

The information that doesn't pass the objectivity test is called misinformation. Sources that provide biased misinformation may still be useful for intelligence analysis. It is possible for misinformation to provide valuable information about a group, an event, or a situation (CMPA, 2002).

Misinformation can be as useful as a source reporting objective facts because these people are espousing untruths for a reason and part of intelligence work is trying to understand all aspects of an event or situation. For this reason, the analyst should not automatically discount misinformation, but use a different measuring stick when reading from it (CMPA, 2002).

An Example of Intelligence Analysis

Data Analysis is an important part of the Intelligence Process due to the analysis of large amounts of collated raw data. Part of the process in understanding the relationships between identities, businesses, locations, motor vehicles, and so on, is the charting of this information in an Association Chart, which is also known as a Link Diagram.

Association Charting provides a graphical representation of the gathered intelligence. Viewing a chart is much easier in understanding the identity relationships and criminal activity than reading through volumes of Information Reports, Briefing Papers. For instance, on page 179 of Volume IX of the Warren Commission Hearings the following testimony of George de Mohrenschildt appears as in Appendix A. The same information becomes a chart, as seen in Appendix B, as result of intelligence analysis.

It is obvious that viewing information on an Association Chart is an easier method of remembering and understanding the pertinent information from a large quantity of text, even though in this example the chart's raw data is sourced from only one page of text. There will be gaps in our knowledge but these will be ascertained and charted at a later stage.

Intelligence Dissemination

Since the U.S. intelligence collection effort is vast and distributed across a number of different organizations, the effort to produce finished intelligence is extensive and involves a number of organizations and results in a large array of intelligence products respectively.

The intelligence products produced by the intelligence organizations mentioned in chapter two can be categorized in two ways. First, according to their designated consumers: national products (for the President and the National Security Council), departmental products (for the Departments of State, Defense, and Energy), and military service/ military commands products (for the Army or the European Command) (Johnson, 1996).

The second method available for categorizing intelligence outputs is by the nature of the product: current intelligence, warning intelligence, estimative and analytical intelligence, periodicals, and databases and maps. This approach is more reflective of reality because the consumers for many products include individuals spread across the government. For instance, an analyst who is responsible for producing finished intelligence on nuclear proliferation or a policymaker who helps formulate decisions in the area may receive intelligence reports from the intelligence components of the

National Intelligence Council, the Joint Atomic Energy Intelligence Committee, the CIA, the DIA, and the Department of Energy as well as other organizations. The analyst's report, wherever he or she is located, may find its way not only to departmental readers but also to those in other departments and levels (Richelson, 1999).

Current Intelligence

Current intelligence is intelligence relevant to a topic of immediate interest like a terrorist attack in Israel. Such intelligence is generally conveyed without the opportunity for prolonged evaluation that is possible in other types of reports. Mostly, it is a product based on one or two sources rather an all-source product (Richelson, 1999).

The President's Daily Brief (PDB)

The PDB is the most restricted and sensitive current intelligence publication of CIA. The PDB is modified to meet the daily intelligence requirements as defined by the President. It contains information from the most sensitive U.S. sources (Central Intelligence Agency [CIA], 1995).

The National Intelligence Daily (NID)

The NID is issued in magazine format six days a week by the CIA's Directorate of Intelligence, in consultation with the DIA, the INR, and the NSA, to emphasize the more important items and to offer its readers a choice between a headline summary and in-depth reports (Hulnick, 1988).

The NID is distributed to hundreds of officials nationwide and some versions of it are cabled to major U.S. military commands and selected U.S. posts overseas (Meyer, 1980).

Daily Economic Intelligence Brief (DEIB)

DEIB is a CIA prepared, five-days-a-week compilation of articles on economic issues of current significance. The brief is tailored to meet the requirements of senior economic policymakers at the cabinet or deputy secretary level (CIA, 1995).

Secretary's Morning Summary

Secretary's Morning Summary is produced by the State Department's Bureau of Intelligence and Research seven days a week. It includes brief reports with comment and three or four longer articles related to policy issues. In addition to its dissemination within the State Department, it is also disseminated to the White House, the National Security Council, and key ambassadors (CIA, 1995).

The Military Intelligence Digest (MID)

MID is the Defense Department's premier current intelligence product. It is produced in a magazine format and published on weekdays. The MID is a joint DIA - military service intelligence and unified command publication that contains items likely to be of interest to national-level policymakers on military or military-related topics. General issues covered include regional security, nuclear security and proliferation, and strategy and resources (McFarland & Zwicke, 1996).

Defense Intelligence Terrorism Summary (DITSUM)

The DITSUM is a product of the Defense department. It is a collection of information and analyses concerning terrorist threats and developments that could affect DOD personnel, facilities, and interests. DITSUM articles include brief terrorism notes, regional terrorism developments, and in-depth special analyses. It also contains a monthly terrorism review by combatant commands. The DITSUM is distributed Monday through Friday in the Washington area in hard copy form and in an electronic message version to military commands outside the area (CIA, 1995).

The SIGINT Digest

This is distributed in hard copy form on weekdays in the Washington area, and electronically to customers in the field, and contains the most significant daily intelligence derived from SIGINT (CIA, 1995).

The World Imagery Report

This is a video-format compilation of current intelligence items derived from imagery collection (CIA, 1995).

Military related products

The military services and unified commands also produce their own current intelligence products. These are: the Air Force Intelligence Daily, the Air Force Intelligence Morning Highlights, the USSPACECOM Space Intelligence Notes (SPIN), the USSPACECOM Strategic Posture Aerospace Threat Summary (SPATS), and the USSPACECOM Intelligence Report (AFIA, 1990).

Current intelligence may also be conveyed by video rather than paper or electronic formats. The DIA distributes finished intelligence via television through the Defense Intelligence Network (DIN), known formally as the Joint Worldwide Intelligence Communications System. For approximately twelve hours a day, five days a week, the DIN broadcasts Top Secret reports to defense intelligence and operations officers at the Pentagon and nineteen other military commands in the United States (Lardner & Pincus 1992).

Warning Intelligence

Warning intelligence products “identify and focus on developments that could have sudden and deleterious effects on U.S. security or policy”(CIA, 1995).

The Warning Watchlist

Among the national-level products that are dedicated specifically to warning intelligence is The Warning Watchlist, a weekly report that tracks and assigns probabilities to potential threats to U.S. security or policy interests in the following six months (CIA, 1995).

Warning Memorandum

It is a product that can be initiated by the National Intelligence Officer for Warning or, through that office, by an element of the intelligence community. The memorandum is a special warning notice that focuses on “a potential development of particularly high significance to U.S. interests.” It is forwarded to the DCI and simultaneously to the principal members of the National Foreign Intelligence Board for a telephone conference, a process that is completed within several hours. The DCI must then decide whether to disseminate the memorandum to policymakers, to commission a National Intelligence Estimate on the subject, or both (CIA, 1995).

Monthly Warning Report

Another national-level product is the Monthly Warning Report for the CINCs, which is a summary of key warning issues that have arisen in intelligence community meetings over the previous month (CIA, 1995).

The Defense Intelligence Agency also issues a number of regular and special warning reports designed to guide U.S. commands around the world. These are: The

Weekly Intelligence Forecast, and the Weekly Warning Forecast Report which include assessments from the various commands; The Quarterly Warning Forecast which reviews a wide range of potential events that could affect U.S. security interests.

These forecasts are distributed in hard copy to members of the Defense Warning System and other decision-makers in the Washington area and in message form to other consumers (CIA, 1995).

Estimative and Analytical Intelligence

National Intelligence Estimates (NIEs)

NIEs are the best-known estimative intelligence products that attempt to project existing military, political, and economic trends into the future and to estimate for policymakers the likely implications of these trends.

Based on inputs from the intelligence community, the NIEs are produced by the National Intelligence Council and formally approved by the National Foreign Intelligence Board (NFIB). NIEs are intended for a variety of customers, from the President and the National Security Council to other senior policymakers to analysts (CIA, 1995).

The Defense Intelligence Report

It is also a DIA estimative product and is defined as "a concise report that addresses a topic of interest to senior policymakers and commanders" (CIA, 1995).

Estimative intelligence produced by the State Department's Bureau of Intelligence and Research is mainly found in memorandums circulated within the department.

The Annual Narcotics Intelligence Estimate

The Drug Enforcement Administration produces NIEs which is a compendium of worldwide production, smuggling, and trafficking trends and projections.

The CIA’s Directorate of Intelligence, the DIA, the INR, and other agencies also produce a variety of reports and studies whose main focus is the analysis of political, economic, military, or social matters (CIA, 1995).

Military Service Analytical Reports

The military service intelligence organizations also produce their own analytical reports as they are designated by the DIA within the Defense Intelligence Production Program (CIA, 1995).

Periodicals

A substantial part of the outcome of the intelligence analysis effort is conveyed in a variety of weekly or monthly publications.

The Economic Intelligence Weekly (EIW)

The CIA publishes the EIW, which analyzes major foreign economic developments and trends and is distributed to top and mid-level policymakers.

The offices within the CIA’s Directorate of Intelligence also publish periodic collections of articles, ranging from weekly to monthly, which may have either a regional or topical focus, such as the European Monthly Review, the Arms Trade Report, and the International Energy Statistical Quarterly (CIA, 1995).

The Terrorism Review

It is a monthly publication of the CIA’s Counter-terrorist Center that addresses current trends in international terrorism activity and methods. It also tracks international terrorist incidents (CIA, 1995).

The International Narcotics Review

It is published monthly by the CIA's Crime and Narcotics Center and evaluates worldwide developments related to narcotics.

Peacekeeping Perspectives

It is a weekly journal on multiparty conflict management and humanitarian operations. The State Department's Bureau of Intelligence and Research Center produces it. It provides the government's only comprehensive review of current or projected peacekeeping operations or humanitarian issues (Central Intelligence Agency [CIA], 1995).

There are some other periodicals produced by a variety of departments. Among those the DEA intelligence produces the Monthly Digest of Drug Intelligence and Quarterly Intelligence Trends; The Air Force produces the Air Force Intelligence Weekly; the U.S. Space Command produces the USSPACECOM Defense Intelligence Space Order of Battle (CIA, 1995).

Biographies, Reference Documents, and Databases

Both the CIA and DIA devote extensive effort to prepare biographical sketches of key civilian and military officials, respectively. The sketches serve as both reference and analytical documents, providing basic information on the individual, as well as exploring his or her motivations and attempting to provide explanations for past and likely future actions (Richelson, 1999).

Defense Intelligence Reference Document (DIRD)

It is a series of documents produced by the DIA. A DIRD can be a one-time or recurring (often encyclopedic) study on military forces and force capabilities, infrastructure, facilities, systems and equipment, or associated topics for military planning and operations. A DIRD may consist of foldout wall charts intended as reference aids or be a more typical book-length publication (CIA, 1995).

CHAPTER 4

SELECTED ISSUES OF INTEREST

The September 11th attacks caused problems for the U.S. beyond the expectations of terrorists. For instance, they crippled the U.S. airline industry, shut down the financial markets for four days, stopped America's economy for a full week of production and created $30 billion or more in direct losses. Moreover, the long-term impact of the attacks, such as wasteful spending on enhanced security, and increased transportation costs will continue to affect the U.S. economy in a negative way (Laing, 2001).

On the other hand, approximately 11,000 terrorists, believed to have spent time in al-Qaeda camps, are still missing and there is a strong probability of several sleeper cells located within the U.S. waiting to conduct attacks (Calabresi et al., 2002). Possible future terrorist targets could include nuclear power plants, petrochemical installations, transportation facilities such as ports and major bridges across the Mississippi, high-value manufacturing plants such as microchip fabricators, the server facilities of major Internet backbone companies and government computer centers such as the Social Security headquarters in Maryland. There is also a possibility of al Qaeda detonating car or truck bombs in U.S. residential suburbs (Deutsch & Smith, 2002; Laing, 2001).

One way to prevent future attacks is improving homeland security. According to Laing (2001), another terrorist attack would not only wreak serious damage on the American economy, but also would demoralize the nation who is already in a state of high anxiety. Therefore, immediate action should be taken to improve U.S. homeland security in order to prevent future attacks.

However, no strategy for a war against terror can rely solely on prevention or defense. To be successful in combating terrorism further action is required and suspects should be detained (Betts, 2002). This requires strong intelligence support. Even though the real story of the intelligence failure is still unknown, it is clear that the U.S. could not prevent the September 11th terrorist attacks. History cannot be changed, but further action can be taken to prevent future attacks. Therefore, some of the efforts to improve intelligence capabilities of the U.S. intelligence community will also discussed in this chapter.

Issues About Homeland Security

The September 11th attacks showed critical deficiencies in airport security but there are other areas vulnerable to future terrorist attacks. Countless other areas of homeland security need to be upgraded. Terrorists aren't likely to be deterred. According to Betts (2002), Available intelligence suggests that al-Qaeda operatives want to bring down more airliners and the government is still trying to get serious about stopping them.

Immediately after September 11, the focus of the Bush Administration was to protect the country from further terrorist threats, to assess the resources available for protecting the homeland, and to establish a budget for homeland security (The White House, 2002). For this purpose, the President established the White House Office of Homeland Security (OHS) in October 2001 to deal exclusively with the job of preparing the country for future terrorist threats and to coordinate activities of the responsible agencies. Former Pennsylvania governor Tom Ridge is heading this office. Since its formation, the OHS has become an important advisory body for the President on reorganizing the government (Scardaville & Spencer, 2002).

Since the establishment of the Office of Homeland Security, the Administration and Congress have sought to address a number of serious concerns. The President included innovative proposals in his first homeland security budget, such as, improving the assistance of government to the first responders and improving the nation's medication stocks. New customs programs and agreements with America's trade partners sought to improve commercial security. State and local governments have been integrated into federal security strategies for everyday concerns and special events. A new warning system was developed to communicate information about potential terrorist threats (The White House, 2002).

On June 6th 2002, President George W. Bush called for creation of a Cabinet-level Department of Homeland Security (DHS) to consolidate many of the federal agencies with homeland security missions (Scardaville, 2002). According to Scardaville and Spencer (2002), this consolidation of nearly 100 federal agencies responsible for homeland security into one department is the most extensive restructuring of the federal government since World War II. The Office of Homeland Security, which has been working independently to coordinate federal homeland security policy among the remaining agencies, will work cooperatively with the new Department of Homeland Security (Scardaville, 2002).

Congress has also contributed to homeland security. Congress took strong homeland security measures by enacting laws that are designed to address security challenges facing the country. In fall 2001 the Congress passed and the President signed the U.S.A. Patriot Act (P.L. 107-56) and the Aviation Security Act (P.L. 107-71). In early 2002, the Enhanced Border Security and Visa Entry Reform Act (P.L. 107-173) was enacted. The USA PATRIOT Act gives law enforcement the ability to combat terrorists with 21st century technology. The Aviation Security Act and the Border Security Act aim to make it more difficult for terrorists and their weapons to enter the country (Scardaville & Spencer, 2002). Additionally, the White House released the nation's first homeland security budget to focus government’s power on a number of long-neglected policies (Calabresi et al., 2002).

Despite such progress, a number of key policy areas and vulnerabilities present on September 11th still need to be addressed. For example, federal agencies continue to compartmentalize terror-related intelligence and block rapid access to it. America's police, emergency medical services, fire departments, and public health workers are not adequately prepared to respond to mass casualty terrorist attacks of any type, especially for those using a weapon of mass destruction (Deutsch & Smith, 2002).

There are federally sponsored training exercises that should be conducted for federal, state, and local personnel to help them prepare for all types of emergencies. Because there are only very limited means of detecting the beginning stages of a bio-terrorist attack, a nationwide health surveillance network should be set up to enable local, state, and federal decision-makers to respond in the early stages when rapid responses are most critical (Bergen, 2002).

Even though the National Guard is being uniquely positioned to assist state and local efforts during and after such attacks, the role of the National Guard in homeland security has not yet been adequately defined. The Department of Defense should address the current support of the National Guard to make better able to respond to homeland emergencies without seriously affecting the military (Betts, 2002).

Finally, Congress lacks efficient mechanisms to provide legislative and budgetary oversight of federal homeland security efforts. It should restructure its committees, with new standing committees to complement the establishment of the new Department of Homeland Security (Scardaville & Spencer, 2002).

All of these areas should be top priorities in the near future to focus the federal government's resources more directly on homeland security. To better understand the issues about homeland security, the following selected efforts of the government and recommendations of the experts for improvement are examined in detail.

Homeland Security and the Budget

In February 2002, the President submitted fiscal year (FY) 2003 budget, which includes funding for homeland security. According to Scardaville and Spencer (2002), this is the first budget proposal of a U.S. President that seeks to coordinate and prioritize the homeland security policy.

For 2003, the President has outlined four new initiatives to address areas where federal policies were particularly weak before September 11. These are: using 21st century technology to secure the homeland of the future, supporting first responders, defending against bio-terrorism, and securing America's borders. These four areas account for approximately 55 percent of the $37.7 billion homeland security budget request. They include a tenfold increase in assistance for first responders and a 319 percent increase in bio-terrorism preparedness (The White House, 2002).

The implementation of these initiatives has been supported by the President's FY 2002 Emergency Supplemental Appropriations request. The President has requested $327 million for Federal Emergency Management Agency (FEMA) first responder programs and over $40 million for Department of Justice border security programs. According to Scardaville and Spencer (2002), this type of planning and funding would begin to remedy the traditional lack of resources in these core areas.

As a result of this funding, over a half dozen federal agencies currently operate grant and training programs to support first responders. However, as the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction [Gilmore Commission] (2001) reported, these programs are neither coordinated nor driven by a common goal and this disjointed approach reduces the effectiveness of federal assistance.

While the federal government can do many things to make the nation more secure, many essential tasks remain the responsibilities of state and local governments and the private sector. Instead of dictating what they must do, the Administration is encouraging an active partnership based on cooperation (Scardaville & Spencer, 2002).

Developing a Partnership with State and Local Governments

As noted above, both the President and the OHS director consider the involvement of state and local governments in the development of a coherent homeland security strategy a priority. Improving communications between local, state, and federal authorities, and the private sector will encourage the development of a coherent national strategy and educate officials about what each sector can expect of the other. How a fireman in Nebraska views homeland security may be quite different from how a Washington bureaucrat sees it. Therefore, an agreed upon definition of homeland security is necessary before a strategy can be implemented across all jurisdictional boundaries (Scardaville, 2002).

To facilitate communication and coordination among the federal, state, and local governments, the Administration has established the Office of National Preparedness (ONP) under FEMA. This is an important first step in creating the framework by which local authorities can consult with and receive support from the federal government. Lines of communication are already being put in place. For instance, FEMA sought input from state and local authorities on how it should spend the $3.5 billion reserve for the First Responder Initiative. It held a listening session with over 50 representatives from the first responder community and relevant federal agencies (Federal Emergency Management Agency, 2002).

According to Vigh (2002), since September 11, in two cases: the 2001 Super Bowl and the 2002 Winter Olympics, the Administration has had success in working with local and state authorities to ensure the public safety. In both instances, good planning, cooperation, and proper training resulted in safe events. A total of 5,000 to 7,000 local, state, and federal security personnel were on duty at the Winter Olympics, while at the Super Bowl, about 3,000 individuals, including representatives of the National Football League, the FBI, the Environmental Protection Agency (EPA), the Centers for Disease Control and Prevention (CDC), the Louisiana State Police, the Louisiana National Guard, the New Orleans police, and private individuals, cooperated on security (Peterson, 2002). These successes show the homeland security community, across all levels of government and the private sector, how to train and prepare for large-scale events.

Homeland security goes beyond all levels of government and much of the private sector, and it depends on the cooperation of all involved. According to Scardaville and Spencer (2002), the Administration and Congress should work together to establish a federal team to facilitate state and local strategies that complement the national homeland security strategy. Moreover, the OHS should establish a team of staff members who can travel to the states and local communities to help the local homeland security officials develop and implement plans that complement the national strategy. The team members should be able to work with first responders, public health leaders, and law enforcement officials, in addition to political leaders (Scardaville & Spencer, 2002).

Improving Communication and Warning

In late 2001, the FBI issued a warning to the Governor of California that it had uncovered a credible threat to a number of bridges in that state. The governor took the threat warning to be more severe than the FBI had intended and overreacted (Scardaville, 2002). The failure was neither in the FBI’s warning nor the Governor's response, rather it was in the miscommunication. Similarly, in April 2002, after the FBI had warned banks in the Northeast of potential terrorist attacks, the response was not uniform; some banks closed while others remained open. The FBI failed to coordinate its warning to the banks with a public relations strategy to ensure that the public knew what was happening and how seriously the warning was to be taken (Scardaville, 2002). As seen in the examples, the warnings highlight the need for a well-defined categorization of threats. For this purpose the new Homeland Security Advisory System (HSAS) announced by the director of OHS was created in March 2002 to improve communication between the federal government, state and local officials, and the public (Scardaville & Spencer, 2002). According to Scardaville and Spencer (2002), the HSAS should provide detailed mobilization plans and a coordinated public relations strategy when it considers releasing a general warning. The system should be incorporated into DHS operations, and a permanent office should be established to manage it.

Conducting First Responder Exercises

Part of the $3.5 billion in anti-terrorism grant funding in the President's FY 2003 budget request has been allocated to fund first responder exercises. The federal funding for initial response activities is currently targeted toward 122 of America's most vulnerable cities (The White House, 2002). According to Scardaville and Spencer (2002), What is needed next is for the Administration and Congress to work together to consolidate first responder programs and develop a national training network for state and local first responders. The President's First Responder Initiative is a good first step in improving federal efforts to prepare first responders for terrorist incidents. The Administration should continue to build on this program to ensure that more first responders receive federal training.

Because training exercises are central to learning how to respond to weapons of mass destruction (WMD) events, understanding a jurisdiction's deficiencies, and developing joint response models, training and response exercises should be part of the national homeland security strategy (Bergen, 2002). For this purpose, a task force needs to be established in the Office of Homeland Security to develop a national strategy that includes a more comprehensive training exercise regime. The task force should establish national standards for what constitutes preparedness for chemical, biological, radiological or nuclear (CBRN) events to help officials identify what they must do to be prepared. All first responders, including local law enforcement and public health officials, Emergency

Medical Services, and fire departments, should be included in this initiative (Deutsch & Smith, 2002).

Although the September 11th terrorist attacks were devastating, the resulting destruction was miniscule in comparison to what would occur during a CBRN event in which the entire first response community of a metropolitan area could be killed as well. Therefore, cross-jurisdictional first responder exercises should also be included in the preparedness planning.

These first responder exercises will force authorities at all levels to analyze their capabilities, identify where their responsibility lies, and critique the weaknesses in their response structure. When this information is put together with their goals and performance indicators, local, state, and federal authorities can establish more accurate baselines of preparedness that can be used to identify where future federal funds should be focused (Bergen, 2002).

Finally, DHS should create a center that analyzes and reports the lessons learned from these first responder exercises. A library of lessons learned from exercises conducted by federal and other public or private institutions should be created. All of these materials should be made available to all first responders so they can better prepare for any contingencies and avoid making similar mistakes during their own exercises (Scardaville, 2002). A mechanism is also needed for reporting on the lessons learned from each exercise that can be shared with all communities. Conducting such exercises will be one of the most important aspects of domestic security (Scardaville & Spencer, 2002).

Preparedness for Bio-terrorism

The September 11th and anthrax attacks, made it clear that America's lack of preparedness for biological terrorism is an unacceptable vulnerability (Deutsch & Smith, 2002). Within two months after the September 11th, the Administration requested an additional $1.5 billion for FY 2002 to decrease that vulnerability (U.S. Department of Health and Human Services [HHS], 2001). These funds are being used in building up federal and state pharmaceutical stockpiles, expanding America's smallpox vaccine supplies, expediting the Food and Drug Administration's pharmaceutical development activities, increasing bio-terrorism preparedness at the local level, expanding the response capabilities of the Department of Health and Human Services (HHS), and improving food safety (HHS, 2001).

As the anthrax strike showed early treatment is vital during a biological attack. Therefore, stockpiling vaccines is an essential part of the nation's anti-bioterrorism strategy. According to Scardaville and Spencer (2002), the Administration has been most successful in building up the nation's stockpile of smallpox vaccine. On September 11, the national stockpile was 15.4 million doses, which is inadequate for a population of nearly 300 million people. In November 2001, HHS awarded a contract of $428 million to Acambis Inc. to produce 209 million doses by the end of 2002. In March 2002, a French firm, Aventis Pasteur, announced that it would donate more than 75 million doses stockpiled in its Pennsylvania facility for the past 30 years (Scardaville & Spencer, 2002). Consequently by the end of 2002 there will be more than enough vaccine available to protect all Americans from a smallpox attack. In the event that future terrorists use contagious agents such as smallpox, these vaccines will be instrumental in limiting the outbreak (Scardaville & Spencer, 2002).

According to Scardaville (2002), the Administration and Congress should work together to develop a specific policy for smallpox vaccinations. According to a study at University of Michigan, a vaccination campaign throughout the nation would lead to 200 to 300 deaths and thousands of illnesses (Okie, 2002). On the other hand, if the United States comes under a smallpox attack, the vaccinations would save millions of lives. Therefore, according to Scardaville and Spencer (2002), the Administration should develop an effective vaccination program against smallpox. First responders and members of the public health community should be vaccinated, as they will face exposure to the virus while treating the affected community. Each individual could calculate the risk involved in receiving or not receiving the vaccine.

Policies and strategies should also be developed for the general population such as further research on safer vaccines, and legislation on the issue of liability if people become ill from the vaccine.

Establishing a Health Surveillance Capability

Since September 11, concerns about the ability of terrorists to harm large numbers of civilians with a CBRN agent such as anthrax have focused attention on America's lack of preparedness in this area (Calabresi et al., 2002). To mobilize a rapid response to such attacks, officials must be able to recognize the outbreak of a catastrophic CBRN-related illness or an attack on food and water supplies (Deutsch & Smith, 2002). Early detection and treatment is vital to mitigate the consequences of a biological attack. A biological incident, unlike other terrorist incidents, is not likely to be marked by a visible or audible event because the delivery of a biological agent does not rely on explosives or other distinguishable means of delivery. Instead, a biological attack is more likely to occur by nondescript means, such as through the mail or covert release of an aerosol agent. In fact, in 28 percent of the previous terrorist attacks using chemical or biological agents, the means of dissemination was not identified (Sofaer, Wilson, & Dell, 1999). Recognition that an attack has occurred happens only after a significant number of people start to become sick and an investigation is begun. By this time, many people may have been exposed to the pathogen. Because no such system currently exists to detect such early signs, the United States lacks the necessary resources to coordinate and execute an immediate response plan (Scardeville & Spencer, 2002).

The community of health providers, including doctors, nurses, veterinarians, and public health workers, are the first people in a position to detect an environmental contaminant or biological weapons attack using smallpox, anthrax, or some other agent (Bolton, 2002). The damage of an attack could be reduced significantly if these officials know how to recognize, diagnose, and treat the early symptoms of an outbreak associated with those agents known to be possessed by terrorists or states that support them (Bolton, 2002).

The Bush Administration has taken some important steps to educate the public health community. Its FY 2003 budget request includes over $500 million for preparing hospitals to respond to chemical, biological, radiological, and nuclear (CBRN) events and another $100 million to train and prepare healthcare professionals for terrorism responses (HHS, 2002).

To be able to recognize early on that such an attack has occurred, a number of states, cities, and communities have established municipal or regional health surveillance networks. Kansas City, Missouri; Baltimore, Maryland; Allegheny County, Pennsylvania; and the states of Florida and New Mexico all have established or are developing monitoring and reporting systems (Bavley & Karash, 2002).

Nevertheless, there is no effective way to connect all of these systems into a single national network. Each system is based on different techniques of data collection and distribution therefore there is no compatibility (Bavley & Karash, 2002). It is therefore essential that the federal government develop monitoring standards for state and local health agencies and the health care community, and expedite the development of a national health surveillance network to monitor and disseminate such information. By monitoring and disseminating such information, all levels of government would be better prepared to recognize and respond to an attack in the earliest stages and therefore limit the catastrophic effects (Scardaville & Spencer, 2002).

Strengthening the Borders

All of the 19 terrorists involved in September 11th attacks were able to enter the United States legally and three of them had overstayed their visas. It is clear that the U.S. border is permeable not only to terrorists wishing to enter, but to their weapons, including weapons of mass destruction (WMD) (Flynn, 2002).

The United States cannot completely close its borders. Moreover, stifling immigration and travel contradicts the free and open nature of America's democracy (Scardaville, 2002). On the other hand, conducting comprehensive inspections of every person and cargo container entering the United States is extraordinarily expensive and damaging to the economy. For example, more than 11 million cargo containers enter the United States every year. As of early 2002, less than 2 percent of these cargo containers entering the United States were inspected (Flynn, 2002). Consequently, economic relations with North American Free Trade Agreement (NAFTA) partners, which is valued at nearly $1 trillion, fall in risk as long lines grew at America's ports of entry. Thus, Mexico has seen a 20 percent decline in trade with the United States since September 11 (Scardaville & Spencer, 2002).

Signing Smart Border Agreements with Canada and Mexico in December 2001 and March 2002 is one of the important responses of the US to border the problem. In these agreements the Administration has adopted a multi-pronged approach, relying on both traditional means (such as new immigration regulations and additional border security officers) and innovative approaches (such as using advanced technology, signing new international agreements, and establishing public-private partnerships on security issues) (Scardaville & Spencer, 2002). Both agreements include new intergovernmental customs standards and public-private partnerships to speed non-threatening people and products across the border and allow border security officials to focus on less secure travelers and goods (Scardaville & Spencer, 2002). According to these agreements, companies that enter the program will be permitted on the accelerated inspection lanes at enhanced ports of entry. They must first satisfy the government that their entire supply chain, from manufacturing to the showroom floor, is secure. The first such operational port is in Detroit near the border with Windsor, Ontario. At least 100 companies have already applied to be part of this program (Scardaville & Spencer, 2002).

The U.S. Customs Service recently revealed the Customs-Trade Partnership Against Terrorism (C-TPAT) to provide similar advantages to security-minded foreign companies from nations that trade with the United States. C-TPAT rewards companies that ensure the security of their supply chain by accelerating processing of their products at Customs inspections stations at the ports of entry (Scardaville & Spencer, 2002). This enhanced point-of-origin inspection system would allow Customs inspectors to focus on cargo originating from sources that are a greater risk because their security measures are not known (Scardaville & Spencer, 2002).

While improved security at points of entry will make transporting personnel or material over the northern and southern borders more difficult, terrorists can still use points along America's unguarded borders. To address this, the Smart Border Agreements also include provisions for sharing intelligence and immigration information and coordinating visa and asylum policies (Scardaville & Spencer, 2002).

The Administration also has sought to strengthen federal agencies responsible for securing the border. The President's FY 2003 budget request seeks a significant increase in border security personnel: 1,160 Immigration and Naturalization Service inspectors and 570 Border Patrol agents, as well as a tenfold increase in the federal investment in developing an entry-exit monitoring system (The White House, 2002).

Congress has made border security a priority as well. The USA PATRIOT Act, passed in October 2001, provides additional personnel for securing the northern border, requires a mechanism needed to monitor entry and exit of visa holders, requires the FBI to share more information with the Department of State, and makes it more difficult for terrorists to enter the country and easier to deport them by redefining the definition of terrorist activity for immigration purposes (Scardaville & Spencer, 2002).

In May 2002, the President signed the Enhanced Border Security and Visa Reform Act, which takes the next step in improving border security (Scardaville & Spencer, 2002). Specifically, it authorizes appropriations for additional border security personnel and technology. It requires that the law enforcement and intelligence community better share terror-related information with the Consular Affairs division of the State Department and INS. It establishes additional requirements for INS implementation of an entry and exit monitoring system. It restricts visas to citizens of countries designated as state sponsors of terrorism, reforms the visa waiver program, and establishes a program for monitoring foreign students studying in the United States (Scardaville & Spencer, 2002).

Enforcement of Immigration Laws

Though all 19 terrorists involved in the September 11 attacks had entered the United States legally, a number of them were on federal terrorist watch lists or had overstayed their visas (Scardaville & Spencer, 2002). Since the attacks, the immigration system is still not up to the task of monitoring those who cross the borders. Incredibly, in March 2002, the INS sent notification to two of the dead hijackers: Mohamed Atta and Marwan Alshehhi, that their student visas for flight training had been approved. By September 11, both men not only had completed that training, but also had used their new skills to attack the World Trade Center (Scardaville & Spencer, 2002).

To correct such problems, Congress, the Department of Justice, and the Administration are all seeking to restructure the INS. According to Scardaville and

Spencer (2002), the centerpiece of all three reorganization proposals is a separation of the INS's enforcement and service functions, which all INS officers perform simultaneously at this time. INS Commissioner James Ziglar has already begun implementing internal reforms to streamline management and communications. Even though removing layers of bureaucracy will increase the INS's ability to act more swiftly, it is not enough. New technology must also be obtained to combat terrorism more effectively.

One of the important needs of INS is a mechanism to monitor the entry and exit of visa holders (Calabresi et al., 2002). Currently, once visa holders have entered the United States, the INS has no way to determine whether they leave the country before their visas expire. The INS currently maintains over 80 computer networks that are poorly connected with each other and rarely connected to other federal agencies. According to Scardaville and Spencer (2002), INS's information technology failings complicate accurate record-keeping on immigrants and visitors, as well as information sharing among offices and agencies, and make enforcing immigration law more difficult.

To solve this problem the Congress required the INS to establish an entry-exit monitoring system as part of the Illegal Immigration Reform and Immigrant Responsibility Act (P.L. 104-208) in 1996, but no such system was ever implemented (Fine, 2001). In 2001, the Congress again called on the INS to establish an entry-exit monitoring system in the USA PATRIOT Act and in 2002 in the Enhanced Border Security Act (Scardaville, 2002).

Past efforts to improve INS's computer systems have had only moderate success. The U.S. General Accounting Office and the Office of the Inspector General have been critical of how INS manages technology upgrades (U.S. General Accounting Office, 2000). Further, the INS has not taken measures to ensure that its staff are trained on and utilize the available technology. For example, Glenn Fine, Inspector General for the Department of Justice, testified before Congress that the INS had not adequately trained its employees on the system (Fine, 2001).

Quick and reliable access to information is vital for making good decisions (Betts, 2002). According to Scardaville and Spencer (2002), INS must modernize and simplify its computer networks, and ensure that they are linked to an all-source intelligence fusion center. INS should also train its employees in their uses to meet this objective. On the other hand, the Congress should authorize funds for this purpose as part of the DHS founding legislation.

The Role of the Department of Defense

The Department of Defense has a critical role in protecting Americans from foreign threats (The White House, 2002). It possesses the domestic infrastructure, equipment, and experience to support and train state and local authorities to respond to large-scale attacks on U.S. soil. A Cabinet-level Department of Homeland Security would not take homeland security responsibilities away from the Department of Defense, which will play a crucial support role in the case of a catastrophic terrorist attack (The White House, 2002). However, adequate communications between the two departments are necessary.

The primary military medium of the Defense Department's contribution to homeland security is the National Guard. National guard is the consistent element of the armed forces to act as lead military agency for homeland security (Scardaville, 2002). By law and tradition, the Guard connects local communities to the federal and state governments. Its units are located in every American community and have the capabilities, legal authority, and structure to respond to attacks on the homeland. The Army National Guard has over 3,000 armories around the nation, and the Air National Guard has 140 units throughout the United States and its territories (Scardaville & Spencer, 2002).

However, according to Spencer and Wortzel (2002), when Guard resources are directed toward homeland security, it should be important to ensure that these resources are not wasted on missions better handled by the private sector or other government agencies. For example, the National Guard should not be guarding airports or the nation's borders. Trained police or security personnel can perform that job. National Guard members have specialized training and legal standing that gives them a unique role in homeland security that should not be squandered (Spencer & Wortzel, 2002).

National Guard State Area Commands (STARCs) are well situated to oversee the training of state and local first responders in weapons of mass destruction (WMD) consequence management. They function as management and operational coordinating centers for the National Guard and are located in every U.S. state (Spencer & Wortzel, 2002). Currently, the Guard maintains approximately 30 Civil Support Teams (WMD-CSTs) of 22 Guardsmen trained and equipped to respond to CBRN events. These units could provide valuable training to state and local first responders (Spencer & Wortzel, 2002).

The National Guard could also help state and local authorities understand how to maintain vital equipment and sustain operations in a CBRN environment, and to plan for medical treatment after an attack (Spencer & Wortzel, 2002). Local health authorities are not adequately prepared to address the mass casualties that would result from CBRN events; many would not know, for example, when to enter an environment or stay away, or when to admit patients to a public facility or send them to an off-site secure facility (Spencer & Wortzel, 2002).

According to Scardaville and Spencer (2002), the Defense Department has to work more closely with Canada and Mexico, as terrorist threats against the United States are also likely to affect them or vice versa. Such cooperation with Canada has a long history of success in the North American Aerospace Defense Command (NORAD). However, this cooperation must move beyond air attack and missile warning and into the areas of homeland security, such as mutual responses to attacks, coastal defense, and responses against weapons of mass destruction. Similar arrangements must be made with Mexico (Calabresi et al., 2002).

The Coast Guard (USCG), which is primarily responsible for defending the country's maritime approaches, has done an admirable job of adapting to the post-September 11 political environment. Its National Fleet Concept has enabled it to complement and support the Navy. Therefore, the USCG should be recognized as the lead element in coastal security (Betts, 2002).

In addition, the Pentagon recently established a new force command structure to include the Northern Command (NORTHCOM), giving it responsibility for protecting North America from attack (Betts, 2002).

Improving the Congressional Committee System

According to Scardaville and Spencer (2002), no one congressional committee has responsibility for homeland security. Instead, responsibility is spread across 88 committees and subcommittees. For example, in the House of Representatives, there are 14 full committees and 25 separate subcommittees that claim jurisdiction over some aspect of homeland security. This committee system in Congress complicates the development of homeland security policy because any congressional committee can hold a comprehensive hearing on homeland security budgets and policy (Scardaville & Spencer, 2002).

Thus, it is difficult for the Administration to communicate its plans to Congress. OHS Director Ridge and his staff are forced to spend too much time meeting with committee staff. Therefore, Congress should create standing committees in both the House and Senate for homeland security (Scardaville, 2002). According to Scardaville and Spencer (2002), Congress must develop a system that will allow agency heads and department secretaries to meet with just one committee to discuss their involvement in homeland security. Consequently, the time of the Secretary of DHS and Director of OHS can be better spent developing solutions to security problems than repeating the same message to each congressional committee.

Issues About Intelligence

One way to improve intelligence is to raise the overall level of effort by conducting more federal funds to the related agencies. According to Betts (2002), as a consequence of post Cold War era, the country faced a new set of high-priority issues and regions; therefore, intelligence resources went down as requirements went up. For example, the U.S. used below 3 percent of its gross national product in 2001 in terms of defense and intelligence combined for the first time since Pearl Harbor (Gingrich, 2002).

Therefore, it is technically impossible to meet the worldwide intelligence needs without spending more money (Gingrich, 2002).

Surprise attacks

According to Betts (2002) September 11th is the Pearl Harbor of terrorism. September 11th terrorist attacks came as a surprise and the U.S. intelligence community was caught flat footed. Although the attacks on New York and Washington were unexpected for many, after September 11, intelligence officials realized that some indicators of terrorist attacks had been recognized by those who focus on terrorism, but the evidence had not been sufficient enough to show what or where the action would be (Gingrich, 2002). For example, according to Gingrich (2002), in spring 2001, in the Hart-Rudman report by the U.S. Commission on National Security in the 21st Century, it was predicted that there would likely be a catastrophic terrorist attack on American soil within the next two decades. By summer 2001, it had also become clear to those monitoring Osama bin Laden that al Qaeda was plotting an attack (Dillon, 2002). The only question was when and where. Moreover, the arrests of al Qaeda associates in Yemen and India in June 2001 had revealed plans to blow up the American embassies in those countries, and a propaganda videotape, which circulated widely in the Middle East during the summer 2001, showed bin Laden calling for such assaults (Betts, 2002). A warning was reportedly issued, but not one that was a ringing alarm (Dillon, 2002). According to Betts (2002), this is a very common occurrence.

Betts (2002) explains the reasons why US intelligence system was caught by surprise by giving historical examples of intelligence in conventional warfare. According to Betts (2002), throughout history, surprise attacks often succeed despite the availability of warning indicators. Despite the initial success, history has shown that attackers often fail to win the wars that they start with surprise attacks: Germany was defeated after invading the Soviet Union, Japan after Pearl Harbor, North Korea after 1950, Argentina after taking the Falkland Islands, and Iraq after invading Kuwait. The bad thing is that all of those initial attacks succeed in blindsiding the victims and inflicting terrible losses (Betts 2002).

This pattern leads many observers to blame intelligence officials. After surprise attacks, intelligence investigations usually discover indicators that existed in advance but that were obscured or contradicted by other evidence. However, the fault lies more in the nature of organizational forces, than in the skills of spies (Calabrasi et al., 2002).

One reason surprise attacks can succeed is the "boy who cried wolf" problem, in which the quality of intelligence collection works against its success (Betts 2002). There are often numerous false alarms before an attack, and they weaken sensitivity to warnings of the attack that actually occurs. On the other hand, sometimes the supposed false alarms are not false at all, but instead accurate warnings that prompted timely responses by the victim forcing the attacker to cancel or reschedule the assault. Thus it generates a self-negating insight.

Attacks can also come as a surprise because of an overload of incomplete warnings, which is a particular problem for a superpower with world-spanning involvements. In the spring of 1950, for example, the CIA warned president Harry Truman that the North Koreans could attack at any time, but without indications of whether the attack was certain or when it would happen. The same reports also continually warned Truman of many other places in the world where communist forces had the capability to attack (Betts 2002).

Intelligence may correctly warn of an enemy's intention to strike and may even anticipate the timing but still guess wrong about where or how the attack will occur. For example, the U.S. intelligence was warned in November 1941 that a Japanese strike could be imminent but expected it in Southeast Asia. Pearl Harbor seemed an impractical target because it was too shallow for torpedo attacks. That had indeed been true, but shortly before December 1941 the Japanese had adjusted their torpedoes so they could run in the shallows. Similarly, before September 11, attacks by al Qaeda were expected, but elsewhere in the world, and not by the technical means of kamikaze hijacking (Betts 2002).

The list of common reasons why attacks often come as a surprise goes on and on. The point is that intelligence can rarely be perfect and unambiguous, and there are always several reasons to misinterpret it. Some problems of the past have been fixed by the technically sophisticated system that the US has now, and some may be reduced by adjustments to the system. But some can never be eliminated, with the result being that future unpleasant surprises are a certainty (Betts, 2002).

Sharing The Intelligence Between Agencies

The intelligence community has been the object of increased scrutiny since September 11, with criticism focused largely on the inability of the agencies to predict the attacks (Deutsch & Smith, 2002). However, even if substantial information were available, unless agencies within the intelligence community can share information across departmental and agency boundaries, an accurate assessment of threats to national security is not possible (Dillon, 2002).

Mostly, intelligence analysts deal with a blizzard of information, the vast majority of which appears meaningless in isolation. The analysts are expected to predict both the likelihood and magnitude of future threats. According to Dillon (2002), this is comparable to trying to identify the subject of a jigsaw puzzle before assembling all the pieces. While 10 people may be working to complete the puzzle, they are not sharing the pieces with one another (Dillon, 2002).

Before September 11, various intelligence agencies had identified specific al-Qaeda operatives as possible terrorists (Calabresi et al., 2002). But the problem in interagency communication allowed two people, Khalid Almihdhar and Nawaf Alhazmi, on the Central Intelligence Agency (CIA) watch list to board commercial planes and hijack them (Dillon, 2002). Nawaf Alhazmi was in the United States on an expired visa. The CIA's intelligence on these hijackers was not collated with that of other agencies or made available to the end user. According to Dillon (2002), the Federal Aviation Administration, the agency responsible for screening airline passengers, did not have access to the CIA's database either. According to Scardaville (2002), since no single agency was tasked with piecing together the bits of information on potential terrorists into a single recognizable picture, this failure was possible (Scardaville & Spencer, 2002).

There are numerous agencies and departments at the federal level that either monitor terrorist activity or respond to terrorist attacks. The Department of Justice controls the Federal Bureau of Investigation (FBI), Immigration and Naturalization

Service (INS), and Drug Enforcement Administration (DEA). At the CIA, there is an all-source intelligence collection agency, the Counter Terrorism Center (CTC), which is restricted to collecting foreign intelligence. Federal Emergency Management Agency (FEMA) and the Centers for Disease Control and Prevention (CDC) in the Department of Health and Human Services (HHS) are essential first responders in the event of an attack. The Department of the Treasury and the Coast Guard also have pieces of the counter-terrorism intelligence puzzle (Dillon, 2002).

Moreover, these foreign and domestic intelligence agencies either do not or cannot share intelligence resources as a result of some jurisdictional and bureaucratic barriers. For instance, National Security Act of 1947 (50 U.S.C. 401 note) and Executive Order 12333 of 1981 restrict agencies dealing with foreign intelligence, including the CIA and the Defense Intelligence Agency (DIA), from collecting intelligence on American citizens (Dillon, 2002). According to Scardaville and Spencer (2002), this is a serious problem if an American citizen is involved in the activities of a terrorist group. For example, when a suspected terrorist whom the CIA is tracking enters the United States, the CIA is required to notify the FBI. At that point, either a joint case may be opened or the FBI may allow the CIA to continue its pursuit with its knowledge (Dillon, 2002). In doing its work, the CIA would be able to keep files that include information on U.S. citizens the terrorist interacts, but only as part of a combined CIA-FBI investigation. The CIA, as the key source for the relevant foreign intelligence, would play a crucial role in the FBI investigation. However, once the case was closed (as an investigation) and crucial information turned over for prosecution, the information on American citizens would ultimately have to be removed from CIA files and would no longer be a part of the CIA's intelligence for future all-source analysis and fusion (Harding, 2002).

How that information was collected is another issue. The foreign intelligence community guards its sources and methods of collecting intelligence. Its agencies do not want to share information gathered by electronic monitoring devices or to risk the lives of informants and agents who provide information on terrorists. On the other hand, the law enforcement community gathers intelligence in order to present that information as evidence in court. The missions, methods, and philosophies of the two types of agencies are in conflict as the foreign intelligence community insists on protecting its sources and methods while the law enforcement agency (LEA) gathers intelligence to use it as evidence in court, as result of the constitutional right of an alleged terrorist to face his accuser (Taylor, 1987). According to Dillon (2002), this conflict has been resolved in cases involving spies; it must be resolved with regard to collecting intelligence in the war against terrorism as well.

According to Dillon (2002), if U.S. intelligence gathering is to be effective, the federal government must be able to look at all available pieces of the terrorism puzzle and provide the President with a comprehensive and timely analysis. Intelligence fusion for the country is currently the responsibility of the Director of Central Intelligence (DCI), who has the resources of a Community Management Staff (CMS), a dedicated Deputy for Collection, and a dedicated Deputy for Production. Although the CMS is responsible for making organizations share intelligence, before September 11, the CMS and the primary agencies of the intelligence community (the CIA, the FBI, and the Departments of Defense, Treasury, Energy, and State) failed to ensure intelligence sharing. With the Office of Homeland Security, the proposed Department of Homeland Security is now charged with the responsibility of sharing homeland security-related intelligence (Scardaville & Spencer, 2002).

The President has proposed a number of new policies to promote such information sharing. The most important is a new center to fuse and analyze terrorism-related intelligence within the Department of Homeland Security. The fusion aspect of this center would remedy part of the problem of compartmentalization that still characterizes the collection of intelligence. The fusion center will ensure that intelligence is not only collected and analyzed, but also disseminated to appropriate federal, state, and local agencies with homeland security missions, including the FBI and CIA (Scardaville & Spencer, 2002; Scardaville, 2002).

Other steps taken after September 11 include daily briefings of the President by FBI Director Robert Mueller and DCI George Tenet. Each now knows what is at the top of the other's agenda. In addition, federal intelligence agencies conduct two secure videoconferences each day to discuss information related to terrorist threats.

Intelligence Fusion Center

As mentioned above, in October 2001, Executive Order 13228 established the Office of Homeland Security (OHS), which was tasked to "identify priorities and coordinate efforts for collection and analysis of information" regarding terrorist threats inside and outside the United States (Scardaville, 2002). This is a good first step that will improve information sharing at a number of levels. To this end, according to Dillon (2002), the United States should create an all-source intelligence fusion center that can access intelligence information gathered by the foreign intelligence community as well as domestic intelligence collected by the FBI and local law enforcement agencies (LEAs).

The purpose of an intelligence fusion center is to break down bureaucratic cultures that keep the information away from those who need it. By pulling together information from all the related intelligence agencies, the fusion center can meet that goal (Dillon 2002).

Several existing domestic systems can presumably provide intelligence to a counter-terrorist fusion center. For example: The FBI maintains the National Crime Information Center (NCIC) computer system, to which police officers nationwide have access. The FBI also has the Awareness of National Security Issues and Response (ANSIR) program, which is designed to work closely with businesses and to alert employees of unclassified national security threats (Dillon, 2002). Moreover, the DEA participates in the Organized Crime Drug Enforcement Task Force (OCDETF), which promotes a coordinated effort among all drug enforcement agencies (Dillon, 2002). However, none of these organizations has an all-source collection and analysis capability that covers both foreign and domestic intelligence. Therefore, they do not ensure that all necessary information will reach all decision-makers in a timely fashion (Scardaville & Spencer, 2002).

To ensure that, according to Eggen (2002), all federal terrorism officials must have access to the full scope of government information related to cases they are investigating. The fusion center can include collaborative workspaces manned by analysts from each agency. Collaborative workspaces would allow the various agencies to participate actively in the analytical process while permitting intelligence agencies to protect their sources. According to Dillon (2002), there are technical means and institutional methods for building firewalls or filters between agencies that permit relevant data to be exchanged between intelligence agencies without compromising the privacy of American citizens or forcing substantive changes in the collection of foreign intelligence or law enforcement agency (LEA) information.

To be effective, Dillon (2002) argues that the intelligence fusion center must have the capability to maintain a combined intelligence database. Accordingly, contributing agencies should be able to access this information as needed, based on the assessment of the intelligence fusion center. For example, if a previously identified terrorist attempted to apply for a visa at the U.S. embassy in Yemen, the request would be blocked because the application would have to clear the intelligence fusion center's all-source database (Dillon, 2002). Similarly, whenever the INS processed a visa application, the information could first be verified with the intelligence fusion center (Dillon, 2002).

On the other hand, one intelligence organization cannot discover or uncover every foreign or domestic terrorist attack. The fusion center should not duplicate the activities of existing agencies, but should enhance and improve their efforts by providing a service that does not yet exist. All existing intelligence and law enforcement agencies must continue to bear full responsibility for watching and reporting on their areas of responsibility. The intelligence fusion center would be designed to make the job of finding terrorists easier, not to take the responsibilities of other agencies (Dillon, 2002).

As a result, the new Department of Homeland Security should have an intelligence fusion center that brings together intelligence and law enforcement information from across the entire federal government, analyzes it, and shares it on an as-needed basis. That fusion center should also work closely with the FBI and CIA, which should remain independent of the new department because of their broad missions that extend beyond counter-terrorism (Scardaville & Spencer, 2002).

Dissemination of Intelligence to Local Law Enforcement Agencies

The establishment of an intelligence fusion center would give the President and Director of OHS the tools needed to fuse intelligence collection and analysis at the federal level. However, that accomplishment would complete only half the goals of the executive order that established the Office of Homeland Security (Scardaville & Spencer, 2002). The Director of OHS is also charged to "work with Federal, State, and local agencies as appropriate, to...facilitate collection from State and local governments and private entities of information pertaining to terrorist threats or activities within the United States." To accomplish this goal, the OHS must also break down the vertical barriers between agencies to facilitate vertical and horizontal information sharing (Dillon, 2002).

As seen in September 11th terrorist attacks, local government is the key first responder to acts of terror. In order to protect the homeland from further terrorist events, appropriate planning and threat assessments must be conducted with regard to incoming intelligence information. This planning is best done by state and local governments but it necessitates access to information that has been disseminated only at the federal level. Although the FBI maintains some systems that presumably allow the nation's 650,000 state and local police officers to contribute to homeland security, the intelligence fusion center and federal agencies must create additional systems to share information and maximize the efforts of the state and local police rather than a one-way transfer of information (Dillon, 2002).

The most expeditious means of accomplishing that goal is to reestablish LEA intelligence units for state and local governments. Many of these organizations were dissolved in the 1970s because of distortion and isolated abuses of the intelligence they gathered (Dillon, 2002). The President should require governors to create intelligence offices on the state level to gather, analyze, and disseminate intelligence across federal and local levels of government (Scardaville & Spencer, 2002). According to Dillon (2002), the U.S. Attorney General and State Attorney Generals can publish frameworks for activity to prevent the abuse of such centers.

Training of state and local agents can be handled at DOJ's 30 Regional Community Policing Institutes, allowing the focus to remain within the realm of community policing and public safety rather than expanding to domestic spying. LEA intelligence units can serve as a useful interface for vertical communication with the intelligence fusion center (Scardaville, 2002). The structure and funding for such a relationship already exists within the Department of Justice (Dillon, 2002).

Collection

First way to improve intelligence is to do better at collecting important information about terrorists. It can be done by means of technical collection and human intelligence.

Technical Collection

The U.S. spends more than 90% of its $35 billion annual intelligence budget on technical collection. During the past five years, the U.S. spent billions of dollars to build and launch more than half a dozen radar-imaging spy satellites, 60 Predator unmanned aerial vehicles (UAVS), most of which are used in the operations in Afghanistan

(Deutsch & Smith, 2002). However according to Gingrich (2002), the US still has 25 percent less satellites than it needs. The U.S. must make the appropriate additions and do what it takes to be secure. That means more intelligence, a larger personnel force, and more modern systems in order to ensure security (Gingrich, 2002).

Technical collection is invaluable but obtaining this kind of information has become increasingly difficult. For one thing, so much has been revealed over the years about U.S. technical collection capabilities that the targets now understand better what they have to evade. For instance, state sponsors of terrorism may know satellite over-flight schedules and can schedule accordingly activities that might otherwise be observable. They can use more fiber-optic communications, which are much harder to tap than transmissions over the airwaves. Competent terrorists know not to use cell phones for sensitive messages, and even small groups have access to impressive new encryption technologies.

The NSA, the NIMA, and associated organizations can increase technical collection such as satellite and aerial reconnaissance, signals intelligence, and communications monitoring, by buying more platforms, devices, and employing personnel to exploit them.

Human intelligence

The September 11 attacks showed the adequacy of quality human intelligence capability for the U.S. Almost every expert agrees that use of spies is an essential aspect of combating terrorism. According to Deutsch and Smith (2002), increasing useful human intelligence is the most critical ingredient for rooting out secretive terrorist groups.

The best way to intercept attacks is to penetrate the organizations, learn their plans, and identify perpetrators so they can be taken out of action. But it is not done easily. Spying requires great skill and discipline, something that cannot be achieved quickly (Taylor, 1987). Likewise, human intelligence collection cannot be improved overnight. It takes a long time to build a team of experts who understand the language, culture, politics, society, and economic circumstances surrounding terrorist groups.

Building up human intelligence networks worldwide is a long-term project. The U.S. intelligence community has neither ignored human intelligence nor neglected to target terrorist groups such as Osama bin Laden's al Qaeda organization. Strengthening human intelligence has always been a priority of DCIs (Deutsch & Smith, 2002). Improving human intelligence means strengthening the CIA's Directorate of Operations (DO), the main traditional espionage organization of the U.S. government. During the post-Cold War era the DO was working for the country's interests rather than its survival (Betts, 2002). According to Deutsch and Smith (2002), the agency has worked hard to close the language gap and improve recruitment of informants. For example, since 1998, the DO, has been pushing its officers to diversify their language skills. However, according to Calabresi et al. (2002), the agency struggles to employ and train officers with proficiency in other tongues. For instance, in 2001's graduating class of case officers, just 20% had usable skills in non-Romance languages. Accordingly, when the war in Afghanistan began, the CIA had only one Afghan analyst. The lack of qualified intelligence officers on the ground in Afghanistan has forced the U.S. to count on unreliable sources. This deficiency increases the risk of military mistakes, hinders the hunt for al Qaeda leaders and gives Mollah Omar, bin Laden and their fighters time to escape.

Despite its huge and educated population, there are very few genuinely bilingual, bicultural Americans capable of operating like natives in the Middle East, Central and South Asia, or other places that shelter the terrorists (Betts, 2002). Thus in some cases the US intelligence relies on foreign agents of uncertain reliability. For similar reasons there have been limitations on the capacity of translating collected information. The need is not just for people who have studied Arabic, Pashto, Urdu, Dari or Farsi, but for those who are truly fluent in those languages. Money can certainly help here, by paying more for better translators and, over the long term, promoting educational programs to broaden the base of enlists. For certain critical regions of the world, however, there are not enough potential agents; therefore, the U.S. intelligence sometimes employ poorly educated immigrants for these jobs with a risk of errors in translation, that cannot be caught because of lack of resources to cross-check the translators (Betts, 2002).

On the other hand, Betts (2002) argues that it is close to impossible to make a way into small, disciplined, alien organizations like Osama bin Laden's al Qaeda. Furthermore, neither bin Laden nor any other terrorist is likely to divulge a full operational plan to a single individual, no matter how carefully he or she is placed as a source. Consequently, no one should expect breakthroughs even if the US gets more and better spies (Calabresi et al. 2002).

Moreover, HUMINT cannot be separated from other intelligence activities because it depends critically on other intelligence efforts. It must be combined with all other sources of information. According to Betts (2002), a requirement for good human intelligence is a thorough understanding of the sources of terrorism. Much of this kind of information can be obtained from open sources such as local newspapers in the communities that harbor terrorist organizations. Such analytic information is essential for planning collection strategies, successfully penetrating terrorist groups, and mounting covert operations to disrupt terrorist activities and facilities. According to Deutsch and Smith (2002), successful human intelligence operations rely critically on intelligence analysis to focus their efforts.

Furthermore, cooperation between human and technical intelligence, especially communications intelligence, makes both stronger. HUMINT can provide access to valuable signals intelligence, which incorporates primarily voice and data communications intelligence. Communications intercepts can validate information provided by a human source. Any operation undertaken in a hostile environment is made safer if communications surveillance is possible (Calabresi et al., 2002). Currently, the NSA, which is under the authority of the Secretary of Defense, carries out communications intelligence, and the CIA carries out human intelligence, which is under the authority of the DCI. The secretary of defense and the DCI share authority for setting foreign collection priorities. In case of foreign threats within the United States, the FBI has primary responsibility for setting collection priorities (Dillon, 2002). According to Scardaville and Spencer (2002), this fragmentation is meaningless when considering the global terrorism threat. The new antiterrorism law took a good first step toward remedying this problem by clarifying the DCI's lead role in setting priorities for wiretaps under the Foreign Intelligence Surveillance Act (FISA) and disseminating the resulting information (Deutsch & Smith, 2002).

Analysis

Intelligence analysis has become the most essential part of intelligence organizations because of the advances in technology and sophistication in types of data and methods of collection (Taylor, 1987). Massive amounts of information have become available more than ever. For example, according to Cahlink (2001), the NSA can collect the equivalent of the entire collection of the Library of Congress in three hours.

The U.S. intelligence community has hundreds of analysts, but there are hundreds of countries and issues to cover as well. Currently, on many subjects the coverage is one analyst per country or issue. When an analyst for a particular issue goes on vacation, or quits, a specialist on something else handles the account temporarily. However, it is hard to know in advance which of the numerous low-priority accounts might suddenly turn into the highest priority. Therefore, Betts (2002) offers hiring more experts and analysts to keep in hand and use them as backup personnel.

Keeping half a dozen analysts on hand for some small country might be a good thing if that country becomes a high priority account or becomes central to the campaign against terrorists. But no good analyst wants to be employed in an inactive account with minor significance because this means most of those analysts would serve their whole careers without producing anything that the U.S. government really needs. Therefore, to make better use of an intelligence analyst reserve corps, Betts (2002) suggests utilizing people with other jobs who come in to read up on their accounts a couple of days each month to maintain currency. If a crisis in their area erupts these people can be mobilized.

It is certain that the quantity of analysts is less important than the quality of what they produce. Investigations of intelligence failures revealed that despite their great knowledge of the situation some analysts failed to predict the disasters (Calabresi et al., 2002). In fact, some of them had warned that an eruption could happen but without any idea of when (Scardaville, 2002). Expertise on a particular subject should result in anticipating a radical departure from the norm. However, the depth of expert knowledge of why and how things have gone as they have require focusing on the same issue for a long time to allow the analyst to estimate whether developments will or will not continue along the same trajectory. Therefore, sometimes analysts don't think that the case will be an exception to the powerful rule, and they underestimate the crisis. At this point Calabresi et al. (2002), offers to encourage "outside the box" analyses that challenges conventional wisdom and consider scenarios that appear low in probability but high in consequence.

However, even if they predict the possible dangers, there is a problem in figuring out what to do with the hypothetical warnings that analysis produces. There are always dozens of equally probable dangers that are possible and paying the costs of taking preventive action against all of them is almost impossible. At this point, Betts (2002) argues that the analysis should be used to identify potential high-danger scenarios for which low-cost fixes are available. For example, if President Bill Clinton had gotten a paper two years before September 11 that outlined the scenario for what ultimately happened, he probably would not have considered its probability high enough to warrant revolutionizing airport security. However he might have pushed for measures to allow checking the lists of flight schools and investigating students who seemed uninterested in takeoffs and landings.

According to Betts (2002), another problem is the full involvement of the analytical units in current intelligence, and leaving no time for long-term research projects. The more farseeing a project, the less likely secret information is to play a role in the assessment (Betts, 2002). This problem can also be solved by using more resources. For instance, there are Middle East experts in think tanks or universities that estimate worldwide trends in radical Islamic movements over the next decade. The intelligence community can have a comparative advantage over outside analysts in bringing together secret information with knowledge from open sources (Betts, 2002).

Today, some of the secrets the CIA needs to pick up are easily accessible, such as the travel plans of the Sept. 11 hijackers. Two of them managed to pay for their airline tickets with credit cards in their own names, even though the CIA had placed them on the terrorist watch list weeks before (Scardaville & Spencer, 2002). Using such open sources by combining them with newly discovered secrets is critical to fighting terrorists. Therefore, the intelligence community should focus on open sources more than ever to be successful (Calabresi et al., 2002).

Conclusion

The terrorist attacks on the World Trade Center and the Pentagon on September 11th 2001, placed homeland security at the top of the nation's priorities. Since then, the President and Congress have done much to meet new challenges to national security, including the proposal to create a Cabinet-level Department of Homeland Security. They also have established budget priorities, quickly enhanced the nation's stockpile of smallpox vaccine, increased security on America's borders, and increased cooperation and communication with state and local government officials.

However, there are some other areas that require additional federal government commitment. For example, Washington should do more to improve dissemination of intelligence between agencies and with state and local authorities. An intelligence fusion center must be created to collect, analyze, and disseminate intelligence on a need-to-know basis. The federal government should expand its CBRN training programs for first responders and establish a national health surveillance network that could detect the presence of a bioterrorist attack at early stages. The Defense Department's role in homeland security should be better defined, especially with regard to the National Guard, which is well-positioned to assume the lead military role in homeland security. Finally, Congress should reform its committee structure to enhance its budgetary, legislative and oversight functions.

CHAPTER 5

CONCLUSIVE REMARKS

Intelligence is one of the world's earliest businesses and it has played an important role in the development of human civilization. Since this research is a descriptive study of the intelligence community and related organizations in the United States of America, it started with a general overview and historical evolution of intelligence in the U.S.

This study has illustrated that there are two fundamental approaches to the purpose and function of intelligence: the traditionalist approach, and the activist approach. The traditionalist approach contends that there should be a boundary between the intelligence producer and policymaker. According to them, the intelligence producer should not be actively involved in policy decisions. On the other hand the activist approach implies a relationship between intelligence and policy, with intelligence producers more actively disposed towards policy objectives and act based upon perceived opportunities. Taylor (1987), adds a third school which is a new version of the activist school that is a result of sophistication in technology, whose main concern is predicting future events, not only to avoid policy drawbacks and political mistakes, by giving accurate information; but, also to plan a course of action for achieving specific goals and objectives.

According to Richelson (1999), the continued major role of U.S. service intelligence organizations is partly a function of bureaucratic politics, partly a function of law, and partly the result of the structure and the requirements of the U.S. military. The structure of the US intelligence community, which is composed of 13 main organizations, is examined under five categories:

1-National intelligence organizations: The Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Imagery and Mapping Agency (NIMA).

2-Department of Defense intelligence organizations: the Defense Intelligence Agency (DIA).

3-Military Service intelligence organizations: Army Intelligence Organizations, Navy Intelligence Organizations, and Air Force Intelligence Organizations

4-The intelligence components of Unified Commands

5-Civilian intelligence organizations: the intelligence offices in the departments of State, Energy, Treasury, Commerce, Justice and Transportation such as INR,OIE, FBI and DEA.

These intelligence agencies conduct five types of intelligence activities: political intelligence, military intelligence, scientific and technical intelligence, economic intelligence, sociological intelligence for the sake of the United States of America.

The intelligence process in the U.S. is examined by using the intelligence cycle. The intelligence cycle is the steps by which information is converted into intelligence and made available to the user. These steps represent sequential phases of planning and direction, collection, processing and production, analysis and dissemination. Planning entails the prioritization of information demands and the allocation of resources. It represents both the first and the last stage. Information is collected from a variety of sources, processed into useful form, analyzed, by drawing upon all available sources to generate balanced conclusions, and disseminated to the consumers of intelligence.

Consumers of intelligence include the President, analysts, national security officials, and others in the executive and legislative branches of government with a need for information to support national security decisions. Dissemination of finished intelligence products may stimulate demand for new requests for intelligence information. Whereas the steps of intelligence cycle usually follow one another in sequence, the function of communication is ubiquitous and takes place continuously throughout the process. Therefore, Betts (2002) describes communication as the lubricant of the cycle.

Of the five steps in the intelligence process, analysis, which entails the conversion of basic information into finished intelligence, is the most important one because more information is now available to the analyst than ever before as a result of the information revolution. To overcome this problem analysts apply all-source analysis to convert collected information from multiple sources into finished intelligence products that are useful to intelligence consumers. It includes integration and evaluation of all available data, finding patterns among fragmentary or contradictory sources, and drawing inferences from incomplete evidence. During this step in the process intelligence agencies pay particular attention to a source's bias, veracity, and timeliness in order to evaluate its usefulness. Other factors to consider include a source's uniqueness, credibility, scope, depth, tip factor, and other costs of getting useful information for intelligence.

The intelligence products produced by the intelligence organizations are examined by categorizing the outputs by the nature of the product: current intelligence, warning intelligence, estimative and analytical intelligence, periodicals, databases, and maps because the consumers for many products include individuals spread across the government.

The surprising terrorist attacks on the World Trade Center and the Pentagon in September 2001 placed considerable attention on intelligence and homeland security. Therefore the following issues about intelligence and homeland security are examined. Since September 11th 2001, the President and Congress have done much to meet the challenges facing the nation, including an important proposal to create a Cabinet-level Department of Homeland Security (DHS), increasing security at the borders, and enhancing cooperation and communication with state and local governments and civil institutions. They also have established budget priorities to improve intelligence and homeland security, and quickly enhanced the nation's stockpile of smallpox vaccine.

However, according to the experts in the field there are some other key policy areas that have not received enough attention of the government. Specifically, to remedy remaining vulnerabilities and further strengthen homeland security. The following recommendations are considered important:

1- Creating a better federal fusion system for intelligence. Such a center should gather, analyze, and share information as needed to appropriate agencies at the federal, state, and local levels. It should work closely with the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA), which should remain independent of the new department since their broad missions extend beyond counter-terrorism.

2- Consolidating first responder programs and developing a national training network for state and local first responders. The President's First Responder Initiative is a good first step in improving federal efforts to prepare the nation's first responders for terrorist incidents. Additional improvements could be made, such as developing a national system of practical educational facilities that unite federal assistance programs in their region by providing training, information on federal grants, and distance learning programs.

3- Developing a comprehensive program of terrorism response exercises. Exercises that simulate weapons of mass destruction (WMD) events are central to preparing for terrorist strikes. Such exercises should be included in a national strategy for first responders developed by a task force, under the support of the new DHS, with representatives from the Office of Homeland Security (OHS), the Department of Defense, state and National Guard units, the Centers for Disease Control and Prevention (CDC), and other agencies.

4- Expediting the development of a national health surveillance network. Since September 11, concerns about the ability of terrorists to harm large numbers of civilians with chemical, biological, or radiological (CBRN) agents have focused public attention on the lack of local preparedness in this area. To mobilize a rapid response to such attacks, officials must be able to recognize early outbreaks of catastrophic illnesses or attacks on food and water supplies. A nationwide network of local surveillance systems must be established to monitor and rapidly disseminate information about such occurrences across all levels of government.

5- Developing a specific policy for smallpox vaccinations. The U.S. will soon have more than enough smallpox vaccine to protect every American. Determining whether each should be vaccinated is the next step. A recent University of Michigan study estimates that such a campaign could result in up to 300 deaths and thousands of illnesses. But it could also save millions of lives should a terrorist attack occur in high-density areas. The Administration should develop an effective vaccination program against smallpox, beginning with first responders and members of the public health community.

6- Expanding the role of the National Guard. As a first responder in domestic emergencies, the Guard is well-positioned to assume the lead military role in homeland security. Moreover, much of the administrative and command infrastructure that is needed to enable the Guard to take on such a role is in place. Title 32, Section 102 of the U.S. Code forces the Guard to focus on providing support services to active forces, and the Pentagon cannot easily extract it from these duties and redeploy units for homeland security without affecting those active forces. Either the active forces roster will have to expand to cover those services, or their commitments decrease. Steps must also be taken to redefine the Guard's mission.

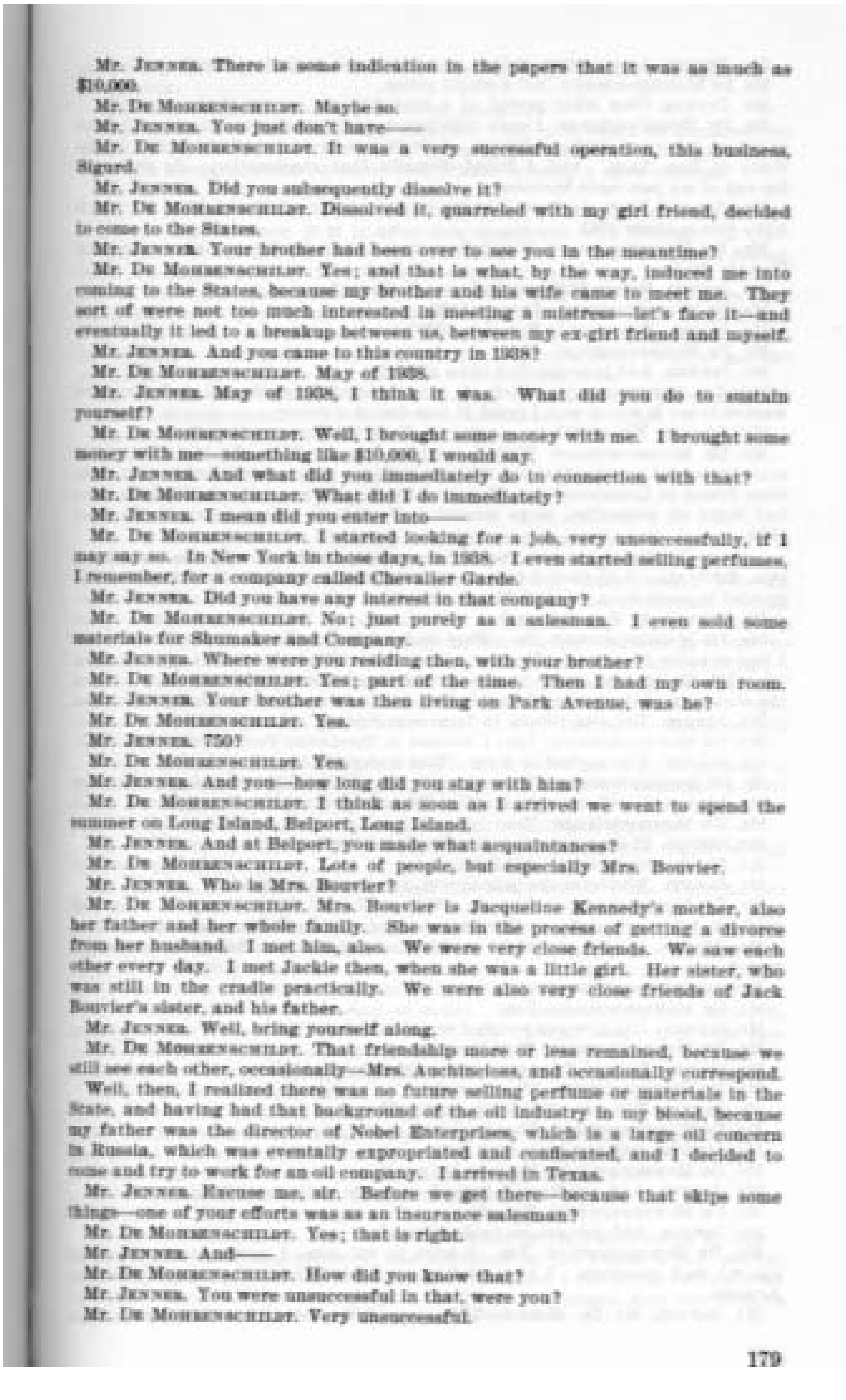
7- Establishing a federal team to facilitate state and local strategies that complement the national homeland security strategy. Homeland security transcends all levels of government and depends on the willing cooperation of all involved. Helping state and local officials make their counter-terrorism plans compatible with the federal strategy will be vital to its success and require close coordination between the new DHS and state and local government officials. OHS Director Tom Ridge should establish a team of staff members who can travel around the country to help local homeland security officials develop and implement plans that complement the national strategy.

8- Establishing standing committees on homeland security in both houses of Congress. Today, homeland security and terrorism-related programs traverse congressional committee jurisdictions. The House alone has at least 14 full committees and 25 subcommittees that claim jurisdiction over aspects of the programs. To complement the creation of a DHS and facilitate Congress's legislative and budgetary role in homeland security, each house should form a standing committee on homeland security with sole jurisdiction for the functions assumed by DHS. Subcommittees should be established to address the departmental divisions proposed by the President: border and transportation security, emergency preparedness and response, CBRN countermeasures, and intelligence analysis and infrastructure protection.

In addition to these, the US intelligence community should increase the level of intelligence collection especially from the point of human intelligence. Moreover, the analysis units should also consider the open sources such as universities and think-tanks while making long term predictions. The intelligence community can have a comparative advantage over outside analysts in bringing together secret information with knowledge from open sources.

As a result, it can be argued that in the twentieth century intelligence played a crucial role in helping to defeat Hitler, in preventing the Cold War from turning into a nuclear war, and keeping the superpower arms race from getting totally out of hand. Even if it looks like terrorism, what impact it will have in the next century cannot now be determined. Intelligence in the hands of those who prefer to avoid war or have a legitimate need to defend themselves can help prevent wars or at least increase the probability that aggressors are defeated. In the hands of those interested in coercion and conquest it is another effective weapon of war (Carmel, 1999; Gannon, 2001; Herman, 1996).

APPENDIX A



Mr. JENNER. There is some indication in the papers that it was as much as $10,000.

Mr. DE MOHRENSCHILDT. Maybe so.

Mr. JENNER. You just don't have——

Mr. DE MOHRENSCHILDT. It was a very successful operation, this business, Sigurd.

Mr. JENNER. Did you subsequently dissolve it?

Mr. DE MOHRENSCHILDT. Dissolved it, quarreled with my girl friend, decided to come to the States.

Mr. JENNER. Your brother had been over to see you in the meantime?

Mr. DE MOHRENSCHILDT. Yes; and that is what, by the way, induced me into coming to the States, because my brother and his wife came to meet me. They sort of were not too much interested in meeting a mistress—let's face it—and eventually it led to a breakup between us, between my ex-girl friend and myself.

Mr. JENNER. And you came to this country in 1938?

Mr. DE MOHRENSCHILDT. May of 1938.

Mr. JENNER. May of 1938, I think it was. What did you do to sustain yourself?

Mr. DE MOHRENSCHILDT. Well, I brought some money with me. I brought some money with me—something like $10,000, I would say.

Mr. JENNER. And what did you immediately do in connection with that?

Mr. DE MOHRENSCHILDT. What did I do immediately?

Mr. JENNER. I mean did you enter into——

Mr. DE MOHRENSCHILDT. I started looking for a job, very unsuccessfully, if I may say so. In New York in those days, in 1938. I even started selling perfumes, I remember, for a company called Chevalier Garde.

Mr. JENNER. Did you have any interest in that company?

Mr. DE MOHRENSCHILDT. No; just purely as a salesman. I even sold some materials for Shumaker and Company.

Mr. JENNER. Where were you residing then, with your brother?

Mr. DE MOHRENSCHILDT. Yes; part of the time. Then I had my own room.

Mr. JENNER. Your brother was then living on Park Avenue, was he?

Mr. DE MOHRENSCHILDT. Yes.

Mr. JENNER. 750?

Mr. DE MOHRENSCHILDT. Yes.

Mr. JENNER. And you—how long did you stay with him?

Mr. DE MOHRENSCHILDT. I think as soon as I arrived we went to spend the summer on Long Island, Belport, Long Island.

Mr. JENNER. And at Belport, you made what acquaintances?

Mr. DE MOHRENSCHILDT. Lots of people, but especially Mrs. Bouvier.

Mr. JENNER. Who is Mrs. Bouvier?

Mr. DE MOHRENSCHILDT. Mrs. Bouvier is Jacqueline Kennedy's mother, also her father and her whole family. She was in the process of getting a divorce from her husband. I met him, also. We were very close friends. We saw each other every day. I met Jackie then, when she was a little girl. Her sister, who was still in the cradle practically. We were also very close friends of Jack Bouvier's sister, and his father.

Mr. JENNER. Well, bring yourself along.

Mr. DE MOHRENSCHILDT. That friendship more or less remained, because we still see each other, occasionally—Mrs. Auchincloss, and occasionally correspond.

Well, then, I realized there was no future selling perfume or materials in the State, and having had that background of the oil industry in my blood, because my father was the director of Nobel Enterprises, which is a large oil concern in Russia, which was eventally expropriated and confiscated, and I decided to come and try to work for an oil company. I arrived in Texas.

Mr. JENNER. Excuse me, sir. Before we get there—because that skips some things—one of your efforts was as an insurance salesman?

Mr. DE MOHRENSCHILDT. Yes; that is right.

Mr. JENNER. And——

Mr. DE MOHRENSCHILDT. How did you know that?

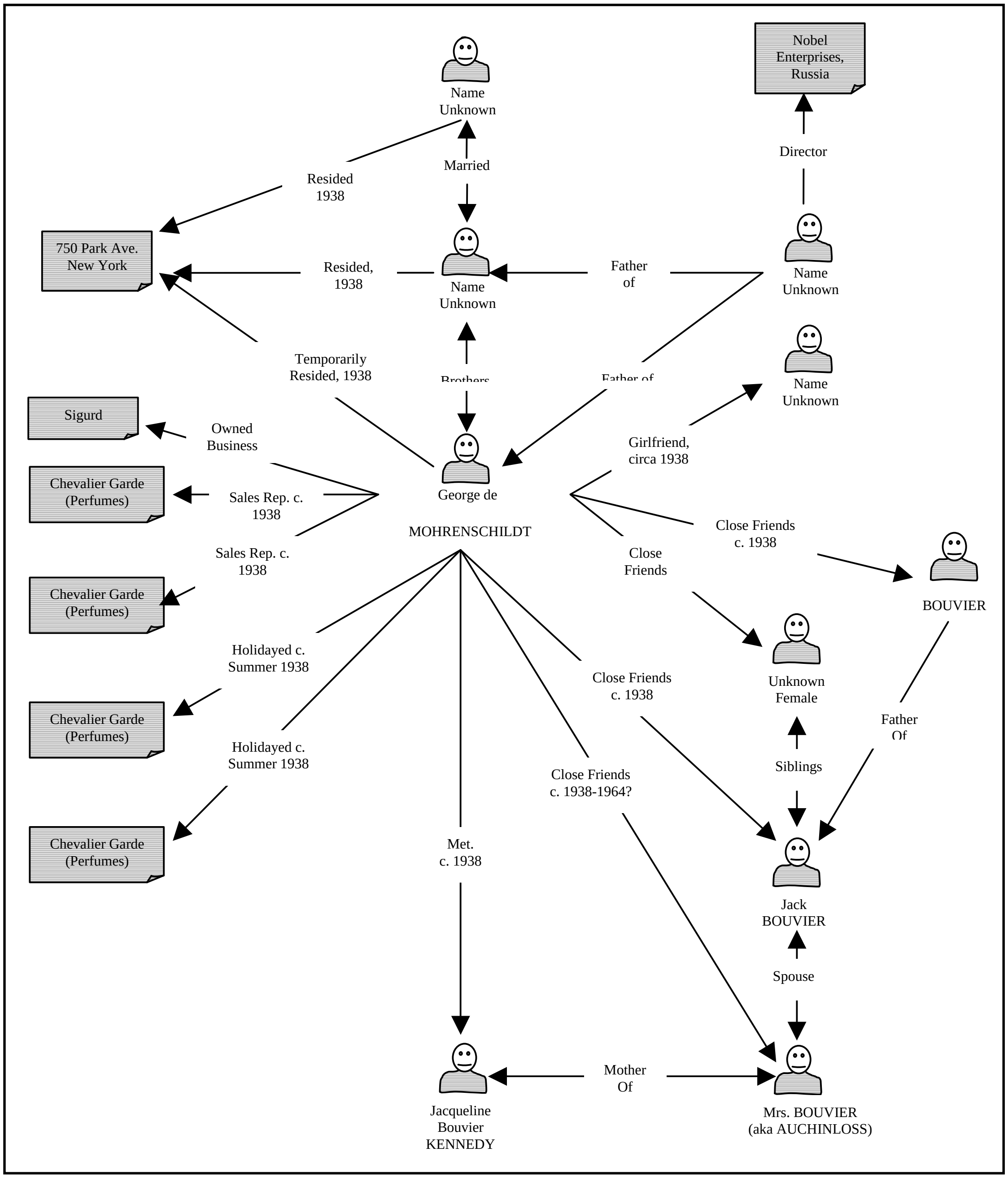
Mr. JENNER. You were unsuccessful in that, were you?

Mr. DE MOHRENSCHILDT. Very unsuccessful.

Source: [http://www.jfklink.com/linkdiagrams/testimony01a.html]

APPENDIX B

Figure 2: Association Chart



Source: [http://www.jfklink.com/linkdiagrams/Jfklink01a.html]

REFERENCE LIST

Adarn, J. A., Zorpette, G., Meyer, S. M., & Horgan, J. (1986). Peacekeeping by Technical Means: Special Report/Verification. *IEE Spectrum*, 23, 42-80.

Air Force Intelligence Agency. (1990, June 7). Organizations and Functions. *AFIAR*, 23-1, F-6.

Air Force Intelligence Agency. (1996, December 3). Air Force Intelligence and Security Doctrine. Retrieved July 18, 2002 from the World Wide Web: http://www.fas.org/man/doctrine.htm#usaf

Bavley, A., & Karash, J. A. (2002, April 23). KC Gets Computer System to Warn of Signs of Bioterror Attacks. *The Kansas City Star*, 18.

Bergen, P. L. (2002). Picking up the Pieces; What We Can Learn From –and About-9/11. *Foreign Affairs*, 81, 2, 169- 175.

Berkowitz, B. D., & Goodman, A. E. (1989). *Strategic intelligence for American National Security*. Princeton, New Jersey: Princeton University Press.

Betts, R. K. (2002). Fixing Intelligence. *Foreign Affairs* , 81, 1, 43- 59.

Bolton J. (2002, May 6). Beyond the Axis of Evil: Additional Threats from Weapons of Mass Destruction. Retrieved June 30, 2002 from the World Wide Web: http://www.heritage.org/Research/MissileDefense/HL743.cfm

Brammer, D. & Hulnick, A. S. (1984). *Intelligence and Policy – The On-Going Debate* McLean Virginia: CIA

Cahlink, G. (2001). Breaking the Code. *Government Executive*, 33, 12, 57-61.

Calabresi, M., Ratnesar, R., McGirk, T., & Ripley, A. (2002, March 11). Can we stop the next attack? *Time*, 159, 10.

Carmel, H. (1999). *Intelligence for Peace: The role of intelligence in Times of Peace.* Portland, Oregon: Frank Cass Publishers.

Central Intelligence Agency. (1995). *A Consumer's Guide to intelligence*. Washington DC : CIA .

Center for Media and Public Affairs (2002, January 17). Retrieved July 18, 2002 from the World Wide Web: http://www.cmpa.com/Links/accuracy.htm

Davis, J. (1992). *The Challenge of Opportunity Analysis* (CSI 92-003U). Washington, DC: Center for the Study of Intelligence.

Deutsch, J., & Smith, J. H. (2002). Smarter Intelligence. *Foreign Policy*, 128, 64-69.

Dillon D. R. (2002, April 10). Breaking Down Intelligence Barriers for Homeland Security.Retrieved May 30, 2002 from the World Wide Web: http://www.heritage.org/Research/NationalSecurity/BG1536.cfm

Eggen, D. (2002, May 22). FBI Pigeonholed Agent's Request. *The Washington Post*, p. A1.

Federal Emergency Management Agency. (2002, April 23). *FEMA Seeks Input on First Responder Grants Program* . Retrieved May 30, 2002 from the World Wide Web: http://www.fema.gov/nwz02/nwz02_36.shtm

Fine, G. A. (2001, October 11). Testimony of Inspector General, United States Department of Justice, before the Subcommittee on Immigration and Claims, Committee on the Judiciary U.S. House of Representatives. Retrieved May 13, 2002 from the World Wide Web: http://www.rppi.org/ps297.pdf

Flynn, S. E. (2002). America the Vulnerable. *Foreign Affairs,* 128, 60-74.

Foreign Broadcast Information Service (FBIS). (2002, July 12). Retrieved July 18, 2002 from the World Wide Web: https://portal.rccb.osis.gov/criteria.html

Gannon, J. (2001). *Stealing Secrets and Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*. Washington, DC: Barsey's, Inc.

Gilmore Commission. (2001, December 15). The Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Retrieved May 30, 2002 from the World Wide Web: http://www.rand.org/publications/IP/IP217/IP217/

Gingrich N. (2001, November 9). The Road Ahead: Securing the Home Front in the 21st Century. Retrieved May 30, 2002 from the World Wide Web: http://www.heritage.org/library/lecture/hl722.html

Godfrey, E. D., & Harris, D. R. (1971). *Basic elements of intelligence.* Washington, DC: U.S. Government Printing Office.

Godson, R. (1989). *Intelligence Requirements for the 1990,s: Elements of Intelligence.* Washington, DC: National Strategy information Center Inc.

Godson, R. (1992). *Intelligence Requirements for the 1990,s: Intelligence Analysis.* Washington, DC: National Strategy information Center Inc.

Gottlieb, S., Arenberg, S., & Singh, R. (1994). *Crime Analysis from first report to final arrest.* California, US: Alpha Publishing.

Harding B. (2002, April 10). Breaking Down Intelligence Barriers for Homeland Security.Retrieved May 30, 2002 from the World Wide Web: http://www.heritage.org/Research/NationalSecurity/BG1536.cfm

Harris, D.R. (1976). *Basic elements of intelligence (Rev. ed.)*. Washington, DC: Government Printing Office.

Hastedt, G. (1991). Intelligence and U.S. Foreign Policy: How to Measure Success? *International Journal of Intelligence and Counterintelligence*, 5, 1, 49-62.

Herman, M. (1996). *Intelligence Power in peace and War*. New York, NY: Cambridge University Press.

Heymann, H. (1985). Intelligence/Policy Relations. In A. Mauer, M. D. Tunstall & J. Keagle (Eds.), *Intelligence Policy and Process (pp.57-66).* London: Westview Press.

Hicks, D.C. (1998). Thinking about organized crime prevention. *Journal of contemporary criminal justice*, 14, 4, 325-350.

Hilsman, R. (1956). *Strategic Intelligence and National Decisions*. Glencoe, Illinois: The Free Press.

Hulnick, A. S. (1986). The Intelligence Producer –Policy Consumer Linkage: A Theoretical Approach. *Intelligence and National Security*,1,2, 212.

Hulnick A. S. (1988, April 7). Letter to Author *CIA Office of Public Affairs*. Retrieved July 18, 2002, from http://www.odci.gov/cia/public_affairs/press_release/archives/1988/index.html

Hulnick, A. S. (1999). *Fixing the spy machine: Preparing American Intelligence for the Twenty-First Century*. Westport, CT: Praeger Publishers.

International Press Institute (2002, July 17). Retrieved July 18, 2002 from the World Wide Web:
http://www.freemedia.at/index1.html

Johnson, L. K. (1996). Analysis for a New Age. *Intelligence and National Security,* 11, 4, 657-671.

Kendall, W. (1949). The Function of Intelligence. *World Politics,* 1, 4, 22-26.

Kent, S. (1969). Estimates and Influence. *Foreign Service Journal,* 46, 18-21.

Laing, J. R. (2001, October 15). The Shadow CIA. *Baron's Chicopee,* 81, 42, 23-27

Laqueur, W. (1985). *A World of Secrets: The Uses and Limits of Intelligence.* New York: Basic Books Inc. Publishers.

Lardner, G. J., & Pincus, W. (1992, March 3). On this Network, All the News Is Top Secret. *The Washington Post,* pp. A1, A9.

Laurer P. (1985). Ethics and Inteligence. In A. Maurer, M. D. Tunstall, & J. Keagle (Eds.), *Intelligence Policy and Process* (pp. 69-87). London: Westview Press.

Mahoney, H. T., & Mahoney, M. L. (1998). *Biographic Dictionary of espionage.* Bethesda, MD: Austin & Winfield, Publishers.

Martens, F.T. (1990). The intelligence function. In P.P. Andrews, & M.B. Peterson, (Eds.), *Criminal intelligence analysis* (pp. 1-20). Loomis, US: Palmer enterprises.

Mauer, A., Tunstall, M., Keagle, J. (1985). *Intelligence Policy and Process.* London: Westview Press.

McCarthey, S. P. (1998). *The Function of Intelligence in Crisis Management Towards and Understanding of the intelligence Producer- Consumer Dichotomy.* Vermont, USA: Ashgate Publishing Company.

McFarland, S. & Zwicke, M. (1996). Providing Insights for Policymakers and Warfighters. *Communique*, 4, 12-13.

Meyer, C. (1980). *Facing Reality: From World Federalism to the CIA*. New York: Harper & Row.

National Intelligence Council. (1997). *Global Trends 2010*. Washington D.C. : NIC p.1

Nelson, H. (1993). The U.S. Intelligence Budget in the 1990s. *International Journal of intelligence and Counterintelligence,* 6, 1, 195-203.

O’tole, G. J. A. (1988). The Encyclopedia of American Intelligence and Espionage. Oxford: Facts on File Inc.

Okie, S. (2002, May 8). Studies Cite Smallpox Vaccine Tradeoff. *The Washington Post,* p. A3.

Peterson, B. (2002, May 8). Security Is Job 1 with NFL's Athletic. NFL Internet Network. Retrieved May 12, 2002, from http://www.superbowl.com/xxxvi/ce/feature/0,3892,4897815,00.html.

Peterson, M.B. (1998). *Applications in criminal analysis: A sourcebook.* London: Praeger.

Ransom, H. H. (1973). *Strategic Intelligence*. Morristown, NJ: General Learning Press.

Richelson, J. T. (1999). *The U.S. Intelligence Community*. Boulder, Colorado: Westview Press.

Rockefeller Commission (1975). *Report to the President on CIA activities within the United States*. Washington, DC: U.S. Government Printing Office.

Scardaville, M. (2002, June 12). Principles for Creating an Effective U.S. Department of Homeland Security. Retrieved May 14, 2002 from the World Wide Web: http://www.heritage.org/Research/NationalSecurity/BG1559.cfm .

Scardaville, M., & Spencer, J. (2002, June 25). Federal Homeland Security policy: A Nine-Month Assessment. Retrieved June 30, 2002 from the World Wide Web: http://www.heritage.org/Research/NationalSecurity/BG1563.cfm.

Scardaville, M., & Spencer, J. (2002, May 13). Meeting the Needs of America's Crucial First Responders. Retrieved May 14, 2002 from the World Wide Web: http://www.heritage.org/Research/HomelandDefense/BG1548.cfm.

Schneider, S. (1994). The criminal intelligence function: Toward a Comprehensive and Normative Model. *Law Enforcement Intelligence Analyst Digest*, 9, 2, 1-26.

Simpson, J. A., & Weiner, E. S. C. (Ed.). (1989). *The Oxford English dictionary* (2nd ed., Vols. 1-10). New York : Oxford University Press.

Sofaer, A. D., Wilson, G. D., & Dell, S. D. (1999). *The New Terror: Facing the Threat of Biological and Chemical Weapons.* Stanford, CA: Hoover Institution.

Spencer, J. & Wortzel, L. M. (2002, April 8). The Role of the National Guard in Homeland Security. Retrieved April 12, 2002 from the World Wide Web: http://www.heritage.org/Research/HomelandDefense/BG1532.cfm.

Steele, R.D. (1993). A Critical Evaluation of U.S. National Intelligence Capabilities. *International Journal of Intelligence and Counterintelligence*, 6, 2, 1993, 173-193.

Taylor, R.W. (1987). Terrorism and intelligence. *Defense analysis,* 3, 2, 165- 175.

The Department of Defense (2002, October 9). The Department of Defense dictionary Retrieved April 12, 2002 from the World Wide Web: http://library.louisville.edu/ekstrom/govpubs/federal/agencies/defense/milterms.html

The White House (2002). Proposal for the Department of Homeland Security. Retrieved July 18, 2002 from the World Wide Web: http://www.whitehouse.gov/deptofhomeland/book.pdf.

The White House (2002). Securing the Homeland, Strengthening the Nation. Retrieved July 18, 2002 from the World Wide Web: http://www.whitehouse.gov/homeland/homeland_security_book.html.

Treverton, G. F. (2001). *Reshaping National Intelligence in an Age of Information*. New York, NY: Cambridge University Press.

U.S. Congress. (1997). *Senate Select Committee on Intelligence, Current and Projected National Security Threats to the United States and its Interests Abroad.* Washington, DC: U.S. Government Printing Office.

U.S. Department of Health and Human Services. (2001, October 17). *Additional $1.5 Billion Proposed to Combat Bioterrorism.* HHS News.

U.S. Department of Health and Human Services (2002, February 5). *HHS Bioterrorism Preparedness Funding Proposal Includes $518 Million for Hospitals, Up 284 Percent*. HHS News.

U.S. General Accounting Office (2000). *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture* (GAO/AIMD-00-212-8).

Vigh, M. (2002, February 1). Superbowl a Dry Run for Law Enforcement. *The Salt Lake Tribune*. Retrieved May 8, 2002, from http://www.sltrib.com/2002/feb/02012002/utah/172522.htm.

Weiner, T. (1998, March 21). Voluntarily, C.I.A. Director Reveals Intelligence Budget. *New York Times*, p. A11

Weiner, T. (2001, October 7). What will the nation's intelligence services have to change to fight this war?. *New York Times*, p. A11.