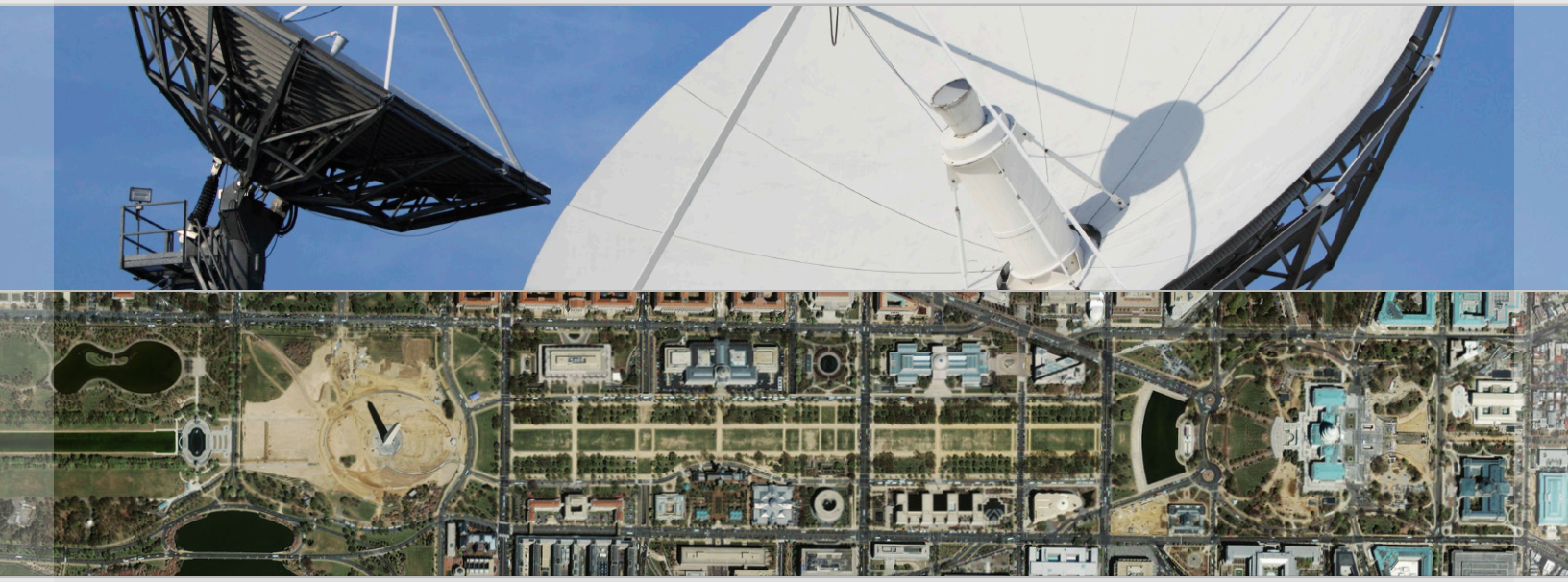
Confrontation or Collaboration?

Congress and the Intelligence Community



Eric Rosenbach and Aki J. Peritz

HARVARD Kennedy School
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

Belfer Center
for Science and International Affairs

Confrontation or Collaboration?

Congress and the Intelligence Community

Eric Rosenbach and Aki J. Peritz

With contributions from Hope LeBeau, Cynthia Lobosky, Ya'ara Barnoon, Susan Sypko, David Tohn, Jessica Reitz, Tamara Klajn, Sarah Miller and JP Schnapper-Casteras.

HARVARD Kennedy School
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

Belfer Center
for Science and International Affairs

The Intelligence and Policy Project
Belfer Center for Science and International Affairs
John F. Kennedy School of Government
Harvard University
79 JFK Street
Cambridge, MA 02138
Fax: (617)495-8963
Email: bcsia_ksg@harvard.edu
Website: http://belfercenter.org

Printed in the United States of America

Design: Tim Duffy

With contributions from Hope LeBeau, Cynthia Lobosky, Ya'ara Barnoon, Susan Sypko, David Tohn, Jessica Reitz, Tamara Klajn, Sarah Miller and JP Schnapper-Casteras.

Satellite image by GeoEye.

Dear Friend,

Your work as a lawmaker is one of the toughest and most rewarding jobs in the country. During the course of your service on Capitol Hill, you will undoubtedly need to consider legislation and issues relevant to national security and the Intelligence Community. Your responsibility to oversee the Intelligence Community will not be easy, but I am confident that you will find extraordinary opportunities to protect and pursue America's interests around the globe.

My friends at the Harvard Kennedy School and I strongly believe that an understanding of the inner architecture of the Intelligence Community will allow you to serve the country more effectively. The Community's size and complexity, however, often confuse and stymie lawmakers attempting to understand intelligence issues. As the 9/11 Commission Report noted, "Few members of Congress have the broad knowledge of intelligence activities or the know-how about technologies employed."

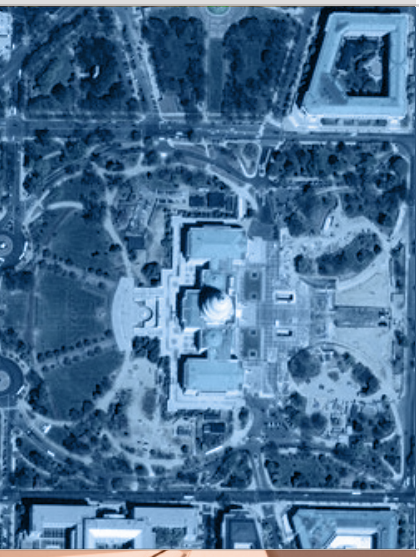
This briefing book attempts to provide you with the foundation to improve your knowledge of intelligence issues. The memos in this book give you important basic information about the Intelligence Community and outline the central issues you will likely encounter during your time in Congress. Although new and unforeseen challenges will certainly arise during your tenure, the ideas presented in this book will provide you with a general framework on many of the issues you will encounter.

I thank you for your service.

Sincerely,

Bob Graham

Table of Contents



Background Memos

Intelligence Basics

Intelligence is a critical tool lawmakers often use to assess issues essential to U.S. national policy. Understanding the complexities, mechanics, benefits and limitations of intelligence and the Intelligence Community (IC) will greatly enhance the ability of lawmakers to arrive at well-grounded decisions vital to our nation's foreign and domestic security.

This memo provides an overview of U.S. intelligence and its primary functions, including intelligence collection and analysis, covert action, and counterintelligence activities.

What is Intelligence?

Intelligence is information that agencies collect, analyze and distribute in response to government leaders' questions and requirements. Intelligence is a broad term that entails:

- *Collection, analysis, and production* of sensitive information to support national security leaders, including policymakers, military commanders and Members of Congress.
- *Safeguarding* these processes and this information through counterintelligence activities.
- *Execution of covert operations* approved by the President.

The IC strives to provide valuable insight on important issues by gathering raw intelligence, analyzing that data in context, and producing timely and relevant products for customers at all levels of national security—from the war-fighter on the ground to the President in Washington.

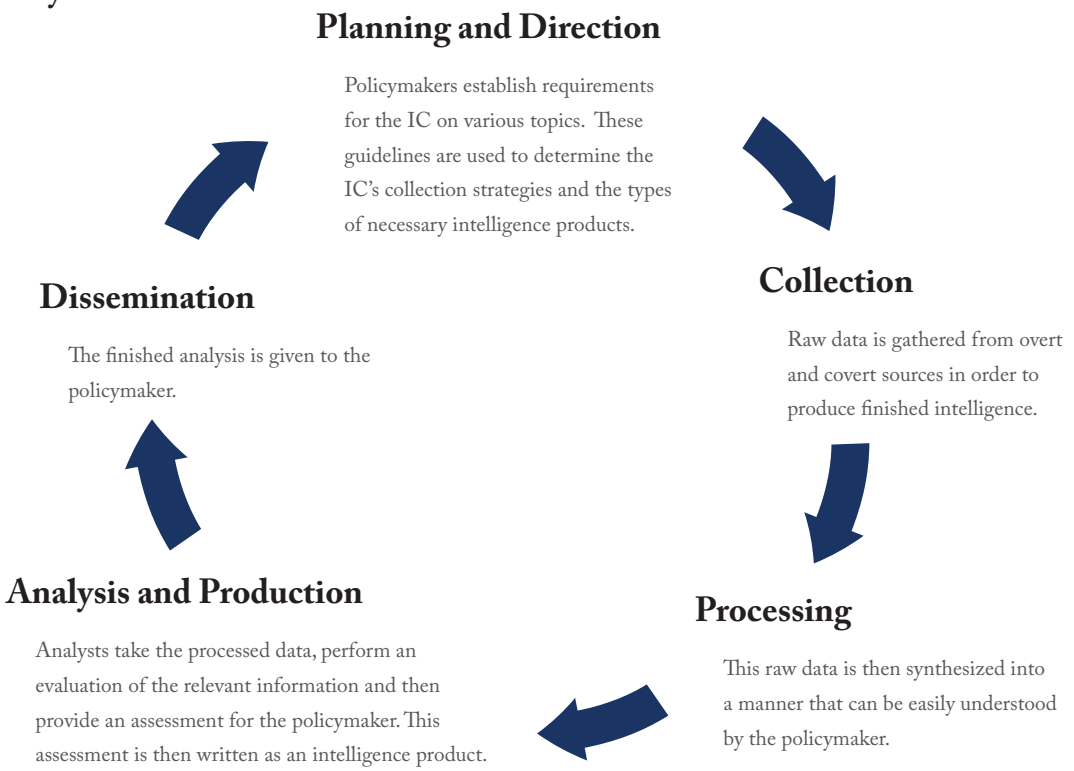
Levels of intelligence include:

- *Strategic*: intelligence needed by policymakers to make policy and military decisions at the national and international level.
- *Operational*: intelligence used by military leaders to plan and accomplish strategic objectives within the operational area.
- *Tactical*: intelligence provided to military leaders in the field to accomplish immediate tactical objectives.

Intelligence Cycle

The intelligence cycle is the process in which intelligence officers convert collected information into valuable intelligence for national security consumers. The cycle begins with establishing priorities and requirements, often with input from policymakers. The cycle then involves collecting, processing, analyzing, and disseminating information for intelligence customers. Some of the most well-known published intelligence products include:

Intelligence Cycle



- *President's Daily Brief (PDB)*, the flagship intelligence product that the Director of National Intelligence delivers every day to the President. This document emphasizes strategic analysis.
- *Worldwide Intelligence Review (WIRe)*, a CIA product that several hundred senior Executive and legislative branch policymakers receive daily.
- *National Intelligence Estimates (NIEs) and National Intelligence Assessments*, products written by the National Intelligence Council (NIC) with input from the entire IC. NIEs often provide a longer-term perspective on issues of critical national security.
- *Secretary of Defense/Chairman of the Joint Chiefs of Staff Daily Intelligence Update (SECDEF/CJCS J2 Daily Intelligence Update)*, a Department of Defense (DoD) product that the DoD leadership receives daily.
- *Secretary's Morning Summary (SMS)*, A State Department product that the Secretary of State receives daily.

Types of Intelligence

Intelligence analysts use five primary disciplines of intelligence collection to draft finished intelligence reports:

Signals Intelligence (SIGINT): Signals Intelligence involves the interception of Communications Intelligence (COMINT) and Electronic Signals Intelligence (ELINT). COMINT is based on information intercepted from messages between individuals, while ELINT refers to the information gleaned from analyzing electronic signals, such as radars.

- The National Security Agency (NSA) has primary responsibility for SIGINT collection and reporting.
- Example: A conversation between foreign adversaries held via telephone is collected by the U.S. using technical means.

Human Intelligence (HUMINT): HUMINT is intelligence collected from human sources, where operations officers and foreign agents conduct clandestine collection.

- CIA's National Clandestine Service (NCS, formerly known as the Directorate of Operations), is the nation's primary collector of HUMINT, though the DoD also conducts HUMINT missions.
- While HUMINT plays a crucial role in the United States' ability to learn more about our advesaries, the IC must carefully scrutinize the information provided by human sources.
- Examples: A U.S. operations officer recruits a foreign scientist to share secrets from that country's nuclear weapons laboratory, or recruits a local tribesman in a conflict zone who provides information on the whereabouts of local belligerents.

Open-Source Intelligence (OSINT): OSINT is based on information in the public domain either domestically or abroad. Sources may include traditional media, Internet forums and media, government publications, and professional or academic papers.

- The Office of the Director of National Intelligence (ODNI) established the national Open Source Center (OSC) in November 2005.
- Examples: Monitoring terrorist video releases, researching military strategy found in foreign "gray" literature, or reading foreign newspapers for insights into adversarial thinking and foreign public opinion.

Geospatial Intelligence (GEOINT): Geospatial intelligence is the visual representation of activities on earth.

- The National Geospatial-Intelligence Agency (NGA) is responsible for GEOINT collection, processing and dissemination. NGA provides GEOINT in all forms, including imagery, imagery

intelligence and geospatial information.

- Examples: A high-resolution satellite photo of a foreign military base with topography and other interactive features, or an unmanned aerial vehicle (UAV) flying over Iraq providing time-sensitive images of insurgent weapons depots for the U.S. military.

Measurement and Signatures Intelligence (MASINT): MASINT is scientific and highly technical intelligence obtained by identifying and analyzing environmental byproducts of developments of interest, such as weapons tests.

- The Central MASINT Office (CMO), a division of the Defense Intelligence Agency (DIA) is primarily responsible for MASINT collection and analysis.
- Example: Sensors help identify types of missiles launched by foreign countries by detecting plume signatures, while other sensors detect uranium particulates in the air or water in order to find foreign nuclear programs.

Covert Action

Defined by the National Security Act of 1947 as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly," covert action is a White House-sanctioned operation that is planned to ensure that the U.S. can mask or plausibly deny its role. Sometimes there are certain unintended consequences of covert action, resulting in negative publicity for the U.S.

- Example: The 1953 coup in Iran, where the U.S. and British intelligence services covertly helped to overthrow Iranian Prime Minster Mohammed Mossadeq, contributed to long-term mistrust and resentment that strains relations between the U.S. and Iran to this day.

Counterintelligence

Counterintelligence (CI) initiatives seek to stymie the efforts of foreign intelligence services (defensive counterintelligence) and manipulate information to confuse foreign intelligence gathering (offensive counterintelligence). The DNI's National Counterintelligence Executive (NCIX) manages the counterintelligence activities of the IC.

- Example of counterintelligence concerns: Foreign agents approaching U.S. businessmen and scientists to learn about U.S. technology advances with military applications.

Organization of the Intelligence Community

The United States Intelligence Community (IC) is a large, sprawling collection of organizations charged with protecting the national security of this country. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 resulted in the IC's largest reorganization in more than 30 years. The IRTPA, for example, created the Director of National Intelligence and the National Counterterrorism Center. In order to assess the efficacy of these reforms, lawmakers must understand the roles of the various agencies in the IC.

This memo provides an overview of the offices and agencies that comprise the U.S. Intelligence Community.

Organization of the Intelligence Community

The Director of National Intelligence (DNI), supported by the Office of the Director of National Intelligence (ODNI), oversees the sixteen government agencies that comprise the IC. Following one of the recommendations of the 9/11 Commission, the IRTPA created the DNI position in 2004.

Office of the Director of National Intelligence (ODNI)

Director of National Intelligence (DNI)

As the cabinet-level head of the IC, the DNI directs and oversees all national intelligence programs. Previously, the Director of Central Intelligence (DCI) led both CIA and the IC. The DNI also serves as principal advisor to the President, the National Security Council (NSC), and the Homeland Security Council on intelligence issues.

Within the ODNI, several interagency centers exist to ensure collaboration across the government on serious threats to national security.

- *National Counterterrorism Center (NCTC)*: The 2004 intelligence reforms designated NCTC as the organization dedicated to integrating the IC's overall counterterrorism efforts. NCTC's mission is to gather and analyze terrorism-related data from across the U.S. government for policymakers, and conduct overall strategic planning against specific terrorist targets.
- *National Counterproliferation Center (NCPC)*: Congress created NCPC in December 2005 to improve efforts to stem the proliferation of weapons of mass destruction and related technologies. The NCPC Director coordinates and identifies intelligence gaps in the U.S. effort to monitor counterproliferation activities.
- *National Counterintelligence Executive (NCIX)*: The NCIX is the center of the government's counterintelligence activities and employs counterintelligence officers from across the IC. Staffed

by counterintelligence (CI) specialists from across the IC, NCIX produces an annual foreign intelligence threat assessment and other analytic products.

- *National Intelligence Council (NIC)*: The National Intelligence Council (NIC) is the IC's center for medium and long-term strategic thinking. Its primary product is the National Intelligence Estimate (NIE), a national security document that contains the coordinated judgments of the IC about topics of high importance.

Central Intelligence Agency (CIA)

The Central Intelligence Agency (CIA) is the lead agency for collecting and analyzing human intelligence, or HUMINT. CIA also produces all-source analysis on a range of national security issues, and is the lead agency for covert action.

Department of Defense (DoD) Intelligence Organizations: Combat Support Agencies

Although the primary mission of the Defense Intelligence Organizations is to support the warfighter, they also work to meet the intelligence requirements of national policymakers.

Defense Intelligence Agency (DIA)

The Defense Intelligence Agency (DIA) provides all-source military intelligence to policymakers and to U.S. armed forces worldwide. The DIA directs and manages DoD intelligence collection requirements for HUMINT and measurement and signature intelligence (MASINT), and provides analysis for signals at (SIGINT) and geospatial intelligence (GEOINT).

National Security Agency (NSA)

The National Security Agency (NSA) collects, coordinates, directs, and performs highly specialized operations to produce—primarily through SIGINT—intelligence and to protect U.S. information systems. NSA supports military customers, national policymakers, the counterterrorism and counterintelligence communities, and key international allies.

National Geospatial-Intelligence Agency (NGA)

The National Geospatial-Intelligence Agency (NGA) provides geospatial intelligence in support of national security objectives. Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on Earth.

National Reconnaissance Office (NRO)

The National Reconnaissance Office (NRO) engages in the research and development, acquisition, launch

and operation of overhead reconnaissance systems. NRO products are used to warn of potential trouble spots around the world, help plan military operations, and monitor the environment.

The Service Intelligence Activities

The intelligence organizations associated with the armed forces focus primarily on operational and tactical issues pertinent to service-specific missions. These organizations include:

- Army: Army Intelligence and Security Command (INSCOM) and the National Ground Intelligence Center (NGIC).
- Navy: Office of Naval Intelligence (ONI).
- Air Force: Air Force Intelligence Agency (AIA).
- Marine Corps: Marine Corps Intelligence Activity (MCIA).
- Coast Guard: Coast Guard Intelligence Coordination Center (CGICC). *

Department of State

Bureau of Intelligence and Research (INR)

The Bureau of Intelligence and Research (INR) serves as the focal point within the State Department for all policy issues and activities involving the IC. INR provides analysis of global developments to State Department officials.

Department of Justice

Federal Bureau of Investigation (FBI)

The Federal Bureau of Investigation (FBI) is the investigative arm of the Department of Justice. It is both a federal criminal investigative body and a domestic intelligence agency. The Directorate of Intelligence (DI) manages all FBI intelligence activities.

Drug Enforcement Administration (DEA)

The Drug Enforcement Agency (DEA) is a law enforcement agency that gathers and analyzes information on drug trafficking. The DEA also pursues U.S. drug investigations outside the country.

Department of Energy

Office of Intelligence and Counterintelligence (OICI)

The Office of Intelligence and Counterintelligence (OICI) analyzes foreign nuclear weapons, nuclear materials, and energy security issues. OICI, known by the acronym IN, also performs counterintelligence analysis on Department of Energy related issues.

* The U.S. Coast Guard is administratively part of the Department of Homeland Security.

Department of Homeland Security

Office of Intelligence and Analysis (I&A)

The Office of Intelligence and Analysis (I&A) focuses on threats relating to border security, chemical, biological, radiological, and nuclear (CBRN) issues, critical infrastructure, domestic extremists, and suspicious travelers entering the U.S.

Department of the Treasury

Office of Terrorism and Financial Intelligence (TFI)

The Office of Terrorism and Financial Intelligence (TFI) protects the nation's financial system and combats the international financial networks that support terrorist organizations, WMD proliferators, the drug trade, and other threats to national security.

Congressional Oversight of the Intelligence Community

Congressional oversight refers to the responsibility of the legislative branch to monitor and indirectly supervise federal programs, agencies, and policies. This authority is rooted in the Constitution's "necessary and proper" clause and the "implied powers" of Congress. Oversight of the Intelligence Community is essential because of the critical importance of ensuring the nation's security, as well as checking the potential for abuse of power.

This memo provides a brief overview of congressional oversight of the Intelligence Community (IC).

Oversight Basics

Congress monitors and regulates intelligence programs and authorizes and appropriates funds. Today, the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) are the primary intelligence oversight bodies on Capitol Hill.

History

These congressional organizations emerged in the late 1970s, when the Church and Pike Committees investigated the CIA and other intelligence agencies in response to the Watergate scandal. Both committees found evidence of spying on American citizens, illegal wiretapping, and cover-ups. As a result, Senate Resolution 400 in 1976 and House Resolution 658 in 1977 established the intelligence committees to prevent future abuses of power and maintain ongoing and regular oversight of the IC.

Membership

The intelligence committees are just one of members' committee assignments. Unlike other committees, positions on the intelligence committees are select assignments made by the leadership on each side in the House and Senate. The 9/11 Commission recommended changes to the intelligence committee structure in the Senate, whereby four of the members would be 'dual-hatted' on the Appropriations, Armed Services, Foreign Relations, and Judiciary committees. Commissioners thought this was important to ensure that the SSCI members included lawmakers familiar with the issues and interests that each of those four committees covers.

- *House Permanent Select Committee on Intelligence (HPSCI)*: 22 members sit on the Committee, although this number has fluctuated in the past. This includes at least one member each from the House Appropriations, Armed Services, Judiciary, and Foreign Affairs Committees.
- *Senate Select Committee on Intelligence (SSCI)*: 15 Senators sit on this committee, although this number also has fluctuated in the past. By rule, the majority party has eight members on the committee, regardless of the number of seats held by the majority in overall Senate. One seat from both the majority and minority party are reserved for standing committee members from

Appropriations, Armed Services, Foreign Relations, and Judiciary. The Chairman and ranking member of the Armed Services Committees serve as ex officio members of the intelligence committees.

Jurisdiction

The congressional intelligence committees maintain jurisdiction over the activities of the 16 members of the IC.

- HPSCI has oversight over both of the programs that make up the intelligence budget, the National Intelligence Program (NIP) and the Military Intelligence Program (MIP). *
- SSCI has jurisdiction over the agencies funded by the NIP.

Shared vs. Competing Jurisdiction

In some cases, the congressional intelligence committees share jurisdiction of certain activities with other congressional committees.

- For example, HPSCI and SSCI share IC oversight with the House and Senate Armed Services Committees. The Senate Armed Services Committee (SASC) conducts oversight over the MIP in the Senate, while the House Armed Services Committee (HASC) shares oversight over the MIP with HPSCI.

In other cases, the congressional intelligence committees compete for jurisdiction over controversial issues that may fall within the purview of additional committees.

- For example, both the Judiciary and Intelligence Committees contend they each had oversight over the once-secret NSA warrantless surveillance program.

Executive and Legislative Give-and-Take

Congress's oversight responsibilities over the IC often overlap with the responsibilities and authorities of the executive branch. Given the natural competition that exists between the legislative and executive branches, this overlap creates tensions as both sides struggle to accomplish certain goals using their respective powers and authorities. Hence intelligence oversight can be one of the most challenging separation-of-powers issues in government.

Executive Branch

The White House sets the national security and foreign affairs agenda. Congress and the judicial branch have affirmed the executive branch's lead role for conducting national security affairs numerous times. Furthermore, the White House can limit congressional influence in the domain of national security and intelligence.

* as explained on p. 24

Access to Information: The White House has the power to control information classification, and even withhold access to information and operational details from certain members of Congress. In this way, the executive branch can directly control what Congress can or cannot see, indirectly influencing the legislative branch's overall ability to make decisions. Thus, despite members of the Intelligence Committees and their staffs holding appropriate security clearances, they may sometimes only have a limited view into specific intelligence activities.

Though the 1947 National Security Act states that Congress must be kept "fully informed" of significant intelligence activities, many Presidents have interpreted this clause to mean they only need to notify the "Gang of Eight" rather than the full membership of the congressional intelligence committees. The Gang of Eight consists of the Senate and House Majority and Minority Leaders, and the Chairs and ranking members of the House and Senate Intelligence Committees.

Veto Power: The President also has the power to veto any legislation that Congress passes. For example, President Bush's veto of the Intelligence Authorization Bill of 2009, which included language on coercive interrogation, indicates that this can be a very effective tool to control the ability of Congress to influence intelligence policy.

Direct Authority: Leaders of the IC are appointed by the President to their positions, and the White House has the authority to hire and fire them. While some of these positions – such as the CIA Director– require Senate confirmation, many do not. As a result, the President is able to appoint trusted advisors to key positions in the IC.

Legislative Branch

Although the Constitution gives the executive branch preeminence in dealing with intelligence matters, Article I nevertheless provides Congress with an important oversight role. However, Congressional oversight into intelligence issues is a complex task, requiring a sophisticated understanding of the issues.

- The floor debate for the FISA Amendments Act of 2008 provided a clear example of the difficulties Congress faces when trying to modify intelligence legislation. Members, for reasons of classification or technical complexity, did not share a common understanding of the law, let alone how it should be adjusted.

Authorization and Appropriation: Congress's most important source of leverage is the power to authorize programs and appropriate funds. During the authorization and appropriations process, Congress can signal its intelligence and policy priorities through both the allocation of funds and the inclusion of non budget-related clauses in the authorization and appropriations bills.

Nominations: Many of the IC's top leaders, including the Director of National Intelligence and the CIA Director, are nominated by the President and confirmed by the Senate. This sometimes grueling

process forces the White House to carefully select its nominees and provides an opportunity for Senate input on both the individuals and issues related to intelligence policy. In recent years, the Senate has withheld confirmation until the executive branch agreed to share additional information on key areas of congressional oversight of intelligence activities.

Congressional Hearings: Congress invites—and, in some cases, compels—high-ranking members of the executive branch to appear before Congress to ask them targeted questions intended to create more transparent and effective IC operations. As noted previously, however, the power of this tool depends in large part on Congress's awareness of IC activities.

Investigations: Congress has responded to perceived intelligence abuses or failures by forming committees and mandating commissions to determine 'what went wrong' and how it might be corrected. In the 1970s, the Church and Pike Committees served this function. More recently, the SSCI conducted extensive investigations on prewar intelligence relating to Iraq.

Treaty Ratification: Treaty ratification is a constitutional power of the Senate. Although few treaties relate directly to intelligence matters, members of the SSCI can use the treaty ratification process to indirectly press related national security policy issues.

Government Accountability Office (GAO): The GAO is the investigative arm of Congress, particularly focused on budget-related issues. As a non-partisan, objective audit and evaluation agency, the GAO gives financial oversight capabilities to Congress. However, classification and security clearance hurdles set by the White House may limit the power of the GAO to investigate intelligence-related topics.

Post-9/11 Intelligence Oversight

The 9/11 Commission concluded that many aspects of congressional oversight of the IC were "dysfunctional." The 9/11 Commission suggested several reforms they assessed would increase Congress's oversight capabilities, including:

- Abolishing term limits for members of the intelligence committees so that they build their expertise to enhance their oversight abilities.
  - Congress implemented this recommendation in 2005.
- Combining the authorization and appropriation functions, thus limiting the number of lawmakers involved and further increasing the efficacy of congressional oversight.
  - Congress has not implemented this recommendation, although the House created an Appropriations Select Intelligence Oversight Panel in 2007. The Panel is comprised of 10 members from the House Appropriations Committee and 3 members from HPSCI. Its primary responsibilities are to review and assess budget requests from the IC and to make recommendations to the relevant Committees and Subcommittees.

Intelligence Oversight Developments

1940 | 1950 | 1960 | 1970

1947 1947

President Harry Truman signs the National Security Act, reorganizing the Intelligence Community and requiring that Congress be kept "fully informed" of intelligence activities.

1956 1956

President Dwight Eisenhower establishes the President's Foreign Intelligence Advisory Board (PFIAB), an independent body to counsel the White House on the "quality and adequacy" of intelligence collection, analysis, and operations.

1975 1975

A Senate Committee, headed by Senator Frank Church, investigates illegal activity on the part of the FBI, CIA, and NSA including the use of warrantless wiretaps against anti-war and civil rights leaders.

March 1976 1976

President Gerald Ford establishes the Intelligence Oversight Board to advise the President on the legality of proposed intelligence activities.

June 1976 1976

The Senate establishes the Senate Select Committee on Intelligence (SSCI) following the conclusion of the Church Committee.

Intelligence Oversight

July 1977 1977

The House of Representatives establishes the House Permanent Select Committee on Intelligence (HPSCI).

1991 1991

Congress passes the Intelligence Authorization Act, which requires the President to inform Congress in writing of all covert actions undertaken by the CIA.

1980 1990 2000 2010

November 1986 1986

The Iran-Contra scandal becomes public.

July 2004 2004

The 9/11 Commission releases its public report, containing approximately 40 suggested reforms, including several to improve Congressional oversight of intelligence activities.

January 2007 2007

The House, responding to recommendations by the 9/11 Commission, establishes the House Appropriations Select Intelligence Oversight Panel to oversee the authorization and appropriation of funding for intelligence activities.

t Developments

The Congressional Authorization and Appropriation Processes

The ability to authorize and appropriate funds provides Congress with a powerful tool for oversight and control of intelligence activities. This "power of the purse," a two-step process of appropriation and authorization over federal spending, provides opportunities for accountability from the Intelligence Community (IC) to Congress. As budgets are drafted and appropriations are made, Congress has the right and responsibility to ensure that the IC spends monies to best meet national security goals.

This memo provides an overview of how the intelligence budget is developed and implemented, as well as how Congress can use the process to influence intelligence and national security policies.

The Intelligence Budget

The intelligence budget funds all intelligence activities conducted by the U.S. government. The budget consists of two parts, the Military Intelligence Program (MIP) and the National Intelligence Program (NIP). Generally speaking, the MIP is devoted to intelligence activities and analysis that support U.S. military operations, most of which are conducted by intelligence agencies in the Defense Department. The NIP includes all other intelligence activities, which predominantly focus on national-level intelligence efforts, but include significant activities conducted by NSA, NGA and NRO.

Following the standard congressional budgetary process, the congressional intelligence committees first authorize funds before they are disbursed by the appropriations committees.

Authorization

Intelligence authorization legislation can establish, continue, or change IC programs and activities. Because of overlapping jurisdiction and shared responsibilities among congressional committees, the process can be long and complex.

From the IC…
The Director of National Intelligence (DNI) begins the process by drafting an initial version of the NIP budget. The DNI works concurrently with the Under Secretary of Defense for Intelligence (USD(I)) to create the initial MIP budget. Those budgets are then submitted to the Office of Management and Budget (OMB) for review and approval. The OMB then forwards the proposals to Congress in the form of Congressional Budget Justification Books (CBJBs).

…to the Hill
The Senate and House simultaneously review the intelligence budget. In the House, the House

Permanent Select Committee on Intelligence (HPSCI) has oversight of the NIP, and shares oversight responsibility for the MIP with the House Armed Services Committee (HASC). In the Senate, the Senate Select Intelligence Committee (SSCI) only has oversight of the NIP, while the Senate Armed Services Committee (SASC) has oversight of the MIP.

- Given the highly technical nature of the authorization and appropriations process, successful authorization bills depend heavily on the work of dedicated budget staffs with extensive knowledge of the IC.

Once the Senate and House Intelligence and Armed Services Committees each have developed and voted on their version of the intelligence authorization bill, which includes budget and programmatic recommendations, the entire Senate and House vote on the bills. Differences between the bills are reconciled in a conference session before the legislation returns to the House and Senate for final passage. Congress then sends the final bill to the President to be signed into law, or vetoed.

Role of Authorization Legislation

The annual intelligence authorization bill does not simply establish the intelligence budget. It also allows Congress to strategically move monies around and to fund new initiatives that Congress believes are necessary. The authorization bill also allows the committees to define intelligence activities, create laws prohibiting certain activities, and press controversial policy issues.

- For example, in response to the Iran-Contra scandal of the 1980s, Congress included a definition of "covert action" in its 1991 intelligence authorization bill that required the congressional intelligence committees be notified of all such activities in writing by the President.
- More recently, the intelligence committees have attempted to use the authorization bills to mandate increased access to information or to press for reform on controversial issues such as interrogation and warrantless surveillance.

Other examples include efforts to declassify the total amount of intelligence budget, as well as an attempt to limit CIA interrogation tactics to those in the Army Field Manual on interrogation. The Bush Administration opposed both efforts and vetoed the 2009 Intelligence Authorization Bill. The President's veto highlights an important point about authorization legislation: If the intelligence committees chose to include policy guidance on controversial issues in the authorization bill, then a veto may deprive Congress of the ability to provide any other explicit guidance to the IC for that year.

- In 2008, Congress faced a difficult strategic choice: Should the bill be sacrificed to highlight an important issue and focus public attention on the President's veto, or should Congress simply ensure passage of the bill that provided important funding and direction to the IC?

Appropriations

The budget process is not complete until the appropriations process provides the actual funding for the activities and programs established through the authorization process. The majority of the intelligence budget appears as a secret lump-sum amount in the Defense Appropriations Bill.

- The House and Senate Appropriations Committees both have Defense Subcommittees, which have jurisdiction over the bulk of the intelligence budget.

The development of appropriations legislation follows intelligence authorization. The subcommittees of the House and Senate Appropriations Committees first draft their own versions, which are voted on in the subcommittee and then within the Appropriations Committee.

- Once the full House and Senate vote on the initial draft, eliminate differences in conference, and vote again on the revised version, the legislation is sent to the President for approval or veto.

Role of the Appropriations Committees

The Appropriations Committees sometimes play a controversial role since the Appropriations Committee can send the IC mixed signals regarding congressional priorities. While the appropriations legislation should follow the intelligence authorization bill, this does not always happen.

- In 1992, for example, the intelligence budget was significantly decreased during the appropriations process.

When the intelligence oversight committees are unable to pass authorizing legislation, they lose a critical oversight tool. For the past several years, intelligence authorization bills have not become law and the Appropriations Committees have included a "specific authorization" clause in the bill to provide IC funding. Essentially, the Appropriations Committees can disburse funds for activities that have not been explicitly authorized by the Senate and House Intelligence Committees.

- Since the Appropriations Committees do not have the same expertise and number of staff focused on intelligence issues, some believe that they may be ill-suited to provide rigorous and comprehensive oversight of the IC.

Reforming the Budget Process

The 9/11 Commission made two recommendations regarding the intelligence budget process that remain issues for debate.

Disclosure of the Budget

The 9/11 Commission proposed that the IC declassify their budget. Although the Constitution

requires the government to regularly release expenditures, the intelligence budget has remained secret for decades. Those supporting disclosure argue that releasing budget figures would eliminate inefficiency and increase government transparency. Opponents claim that disclosing the budget would assist states and groups hostile to the U.S. by providing them with insight to sensitive national security priorities.

- While the Clinton Administration voluntarily released the intelligence budget figures in 1997 and 1998, several legislative attempts to make the intelligence budget public subsequently failed.
- In October 2007, however, Section 601 of Implementing Recommendations of the 9/11 Commission Act of 2007 forced former DNI Michael McConnell to disclose the "top line" of the intelligence budget within 30 days of the close of the fiscal year.

Combining the Authorization and Appropriation Process

Given the complexity of the authorization and appropriations processes, and the importance and unique nature of intelligence oversight, the 9/11 Commission recommended giving the full appropriation function to the intelligence oversight committees. The Commission believed this consolidation would improve congressional oversight of the IC, especially since the best expertise and knowledge about the IC likely resides within the authorization committees.

- The current arrangement may allow the IC to avoid some aspects of oversight and secure funding for programs that may not have explicit authorization.
- Opponents argue that moving appropriations power to the intelligence committees would shift focus from the armed forces to national level intelligence priorities and thus reduce support to the warfighter. Some members of Congress also believe this reform could create an overly powerful intelligence committee.

Informing Congress of Intelligence Activities

Members of Congress cannot monitor the Intelligence Community (IC) without access to information about important and ongoing intelligence activities. In most cases, Congress will have no knowledge of intelligence operations without some level of cooperation with the executive branch. Over the past several decades, the executive and legislative branches have struggled to find the appropriate level of information that should be available to Congress.

This memo provides an overview of the President's obligation to inform Congress of significant intelligence activities—a duty that has taken on renewed importance in light of significant post-9/11 intelligence programs.

Historical Overview

Since the founding of the United States, Congress has long provided oversight of national security and intelligence issues. Examples of this type of oversight include:

- Investigations following the surprise attack on Pearl Harbor during WWII.
- Hearings on Vietnam-era domestic surveillance programs.
- Investigations of pre-war intelligence reports on Iraq's weapons programs.

When Congress passed the National Security Act of 1947—the law that serves as the cornerstone of the modern-day national security apparatus—systematic oversight of the newly reorganized IC was not a priority. After World War II, however, Congress gradually replaced sporadic and ad-hoc investigations with a more regular, organized, and active system of oversight.

Congress eventually formed modern oversight committees, expanded them in the 1970s, and gradually increased their resources. Modernization of oversight mechanisms also resulted in more formal reporting requirements for the executive branch:

- Spurred in large part by the Watergate scandal, Congress in 1974 passed the Hughes-Ryan Amendment to the Foreign Assistance Act of 1961, requiring the President to describe covert activity to the relevant committees in a timely fashion prior to authorization of funds.
- In 1980, Congress passed the Intelligence Oversight Act of 1980 which amended the Hughes-Ryan Amendment. This Act streamlined IC reporting responsibilities to two committees, the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI).

Current Reporting Requirements

The ability of Congress to oversee the intelligence activities of the executive branch is limited by the access that members of the oversight committees have to information about ongoing operations and current intelligence assessments. In an effort to compel the executive branch to provide Congress with information about intelligence activities, Congress adopted in the 1991 Intelligence Authorization bill the modern statutory language that exists today:

> "The President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity…"

When crafting the phrase "fully and currently informed," Congress looked to language used in the Atomic Energy Act of 1946. Congress now interprets this phrase to mean that the IC should affirmatively and proactively report complete, timely, and detailed accounts of intelligence activities.

Covert Action Reporting Requirements

When the President determines that covert action represents the best option for advancing U.S. foreign policy objectives, the law requires him to authorize the covert action through a document called a *presidential finding*. A written finding must be issued within 48 hours after the official policy decision.

- Congress expects that the IC to brief all covert action findings to the full membership of the intelligence oversight committees because they represent *significant intelligence activities*. Furthermore, the National Security Act of 1947 requires the President to report a finding to the intelligence committees "as soon as possible after…approval and before initiation" of the activities.

Extraordinary Circumstances and the Gang of Eight

According to the National Security Act of 1947, the President can limit reporting on significant intelligence activities to a small, select group of members of Congress in "extraordinary circumstances affecting vital interests" of the United States. This select group of legislators is nicknamed the "Gang of Eight," and typically includes:

- The House and Senate leaders from both parties.
- The Chair and ranking members of both House and Senate Intelligence Committees.

The law does not explicitly define "extraordinary circumstances." Nevertheless, Congress intended

that the Gang of Eight exception would apply only to specific time-sensitive covert actions, and *not* all intelligence activities. When passing the 1991 legislation, lawmakers noted that "this provision [should] be utilized when the President is faced with a covert action of such extraordinary sensitivity or risk to life that knowledge of the covert action should be restricted to as few individuals as possible."

If the President finds there are "extraordinary circumstances" and does not immediately inform the committee or the Gang of Eight about the covert action, then the President must still eventually report the activity to the Congress in a "timely fashion" and explain the delay.

- Congress and the White House have disagreed on the meaning of the requirement for reporting in a "timely fashion." Congress generally interprets the requirement as two days, but past Presidents have withheld information for a longer period. This has led to friction between the two branches in the past.

Case Study: The NSA Warrantless Surveillance Controversy

Conflict over presidential reporting obligations, congressional oversight and interpretation of statute surfaced during the recent debate about electronic surveillance. In December 2005, President Bush publicly announced he had authorized the National Security Agency (NSA) to secretly monitor electronic communications without court-issued warrants. The NSA reportedly intercepted the communications of individuals the NSA believed had links to terrorist groups, even if the communication originated, passed through or terminated within the U.S. In the past, collection of these types of communications required a warrant obtained through the Foreign Intelligence Surveillance Court.

The Bush Administration maintained that it fulfilled congressional reporting obligations on the program because:

- The White House briefed the Gang of Eight more than twelve times, affording these members the opportunity to voice opinions or concerns about the program.
- According to Attorney General Alberto Gonzales, the Director of National Intelligence (DNI) only has to inform Congress "[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters."
- It was "common practice" for the White House to inform only the committee chair and ranking member or the "Gang of Eight" for activities similar to the surveillance program.

Members of Congress who wanted full briefings on the NSA program argued that the warrantless surveillance program was not a covert action. Hence, the program did not qualify for limited briefings to the Gang of Eight under the "extraordinary circumstances" exception.

From some lawmakers' perspectives, the administration offered few legitimate reasons for limiting briefings on the program to the Gang of Eight. Furthermore:

- Some members of the Gang of Eight disagreed with the Administration's assertion that they had been given an opportunity to voice their opinion or to disapprove the program.
- Some Bush Administration critics argued that the limited briefings were a deliberate attempt to impede active and effective oversight since the Gang of Eight could not discuss the complex program with legal and technical experts on their staffs.
- The lack of congressional oversight may have harmed the perceived legitimacy of the program.

Covert Action

Covert action is one of many foreign policy tools used by policymakers to advance national interests. Used in select international efforts, covert action encompasses a broad range of activities outside the operations of traditional intelligence collection. Sanctioned by the White House and overseen by Congress, covert action can provide results and otherwise unavailable information.

This memo provides an overview of covert action, including its legal basis, authorization and notification procedures, and historical examples.

What is Covert Action?

According to National Security Act Sec. 503 (e), covert action is, "An activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." Proper covert actions are undertaken because policymakers—*not the intelligence agencies*—believe that secret means are the best way to achieve a desired end or a specific policy goal.

Covert action encompasses a broad spectrum of activities, but may include:

- *Propaganda*: Intelligence agencies covertly disseminate specific information to advance foreign policy goals. United States law prohibits, however, the use of intelligence agencies to influence domestic media and opinion.
- *Political/Economic Action*: Intelligence agencies covertly influence the political or economic workings of a foreign nation.
- *Paramilitary Operations*: Intelligence agencies covertly train and equip personnel to attack an adversary or to conduct intelligence operations. These operations normally do not involve the use of uniformed military personnel as combatants.
- *Lethal Action*: During times of war or armed conflict, the U.S. may need to use covert lethal force against enemies who pose a threat. The U.S. formally banned the use of political assassinations in 1976.

One distinction between covert action and other overt activities, such as traditional diplomatic or military operations, is that U.S. officials could plausibly deny involvement in the activity. This "plausible deniability," however, is predicated upon the covert action remaining secret.

- Example: American involvement in the 1961 Bay of Pigs operation could not be kept secret

once the results became public, so President Kennedy publicly admitted responsibility afterwards at a White House press conference.

A Historically Controversial Tool

Covert action is a necessary—yet sometimes controversial—instrument of U.S. foreign policy. As the challenge of Soviet hegemony emerged as the principal threat to national security, the U.S. used covert action on a wide scale with the goal of combating the threat of worldwide Soviet domination. These efforts resulted in varying degrees of success.

- For instance, in 1954 the U.S. helped overthrow the Guatemalan government in order to prevent the establishment of a perceived "Soviet beachhead" in Central America and to protect U.S. economic interests in the country. This successful coup however, undermined Guatemala's efforts at democratic governance and subsequently led to decades of military rule and civil war.
- On the other hand, congressional inquiries in 1975-76 into Central Intelligence Agency (CIA) actions revealed that the Agency, among other actions, tried unsuccessfully to assassinate foreign leaders and subvert democratically-elected foreign governments.
- The 1987 Iran-Contra affair, which involved the White House's use of non-sanctioned covert action in Iran and Nicaragua in defiance of the law and without proper reporting to Congress, caused further public controversy.

Policymakers still use this foreign policy tool today. For example, covert action was an important device for U.S. national security interests soon after 9/11, as CIA paramilitary groups, U.S. Special Forces and indigenous Northern Alliance forces in 2001-2002 removed the Taliban from power in Afghanistan.

Parameters of Covert Action

U.S. law authorizes CIA to "conduct covert action activities approved by the President." The amended Executive Order 12333 (July 2008) further clarifies:

- The National Security Council (NSC) will "consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action." The NSC is also tasked with conducting periodic reviews of all ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities, as well as consistency with applicable law.
- The Director of National Intelligence (DNI) shall oversee and provide advice to the President

and the NSC with respect to all ongoing and proposed covert action programs.

The Iran-Contra experience led to a more substantial and formalized role for Congress for overseeing and authorizing covert action. In the 1991 Intelligence Authorization Act, Congress established the following procedures for covert action:

- The President must determine, through a document called a *presidential finding*, that a covert action is necessary to support "identifiable foreign policy objectives" of the U.S. A written finding must be issued within 48 hours after the official policy decision which approves the covert action.
- The CIA Director and the heads of all departments, agencies, and entities of the Government involved in a covert action shall keep the congressional intelligence committees fully and currently informed.
- When the President determines that extraordinary circumstances make it essential to limit access to information about the covert action program, the finding may be reported to the Gang of Eight: the chairmen and ranking minority members of the intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and other members of the congressional leadership that the President decides to include.

Examples of Covert Action

Operation Ajax

In 1951, Iran elected Mohammed Mossadeq Prime Minister, who ran under a platform calling for nationalizing the domestic oil industry. At the time, the United Kingdom had considerable oil interests in the country through the Anglo-Persian Oil Company. After the election, Mossadeq nationalized the oil industry, deeply upsetting the British. The U.K., under Prime Minister Winston Churchill then turned to the U.S. to help remove Mossadeq from power. Through a series of covert actions, the CIA worked with the British Secret Intelligence Service to orchestrate the fall of the Mossadeq government and to install the Shah in power in Iran.

For many years, Operation Ajax was viewed as tactically successful, as it achieved the U.S. policymakers' stated goal at the time. However, some suggest the operation was counterproductive and had long-term negative repercussions for the U.S., as the Iranian monarchy fell a generation later to the anti-U.S. clerical regime now ruling Iran.

CIA in Afghanistan 1979-89

Following the Soviet invasion of Afghanistan in December 1979, the CIA launched its largest-ever covert action program to arm the Afghan resistance. During the next ten years, the U.S., Saudi Arabia, and Pakistan provided the Afghans with billions of dollars of weapons and supplies, including advanced anti-aircraft missiles. The armaments and aid proved decisive, neutralizing Soviet air-support in the latter stages of the conflict and eventually causing the Soviets to withdraw from Afghanistan.

In another example of far-reaching consequences, however, a number of the fighters that the U.S. trained and equipped during the 1980s may be fighting American and NATO troops in Afghanistan today.

National Intelligence Estimates

The Intelligence Community's (IC) faulty assessments on Iraqi WMD in 2002 highlights the role Congress plays in promoting the analytic rigor and utility of strategic intelligence assessments, such as National Intelligence Estimates (NIEs). As policymakers and consumers of strategic intelligence, it is also important that members of Congress understand the fundamentals of intelligence assessments and NIEs.

This memo provides an overview of strategic intelligence assessments and NIEs. After discussing the drafting process, the memo highlights challenges the IC faces in NIE production.

What is a National Intelligence Estimate?

National Intelligence Estimates (NIEs) are the IC's most authoritative written judgments on national security issues. NIEs usually provide information on the likely course of future events and highlight the implications for U.S. policymakers.

The National Intelligence Council (NIC) produces NIEs after consulting with all 16 IC members through an interagency process. The NIC serves as a bridge between the intelligence and policy communities, as a source of deep substantive expertise on critical national security issues, and as a focal point for IC collaboration.

- The NIC's goal is to provide policymakers with the best unvarnished and unbiased information, regardless of whether analytic judgments conform to U.S. policy.

Production of a NIE

Senior civilian and military policymakers, including congressional leaders, typically request NIEs.

- Before a NIE is drafted, the relevant National Intelligence Officer (NIO) produces a concept paper or 'terms of reference' (TOR) and circulates it throughout the IC for comment. The TOR defines the key estimative questions, determines drafting responsibilities, and sets the drafting and publication schedule.
- Several IC analysts from different agencies produce the initial text of the estimate.
- The NIC then meets to critique the draft before it is circulated to the broader IC.
- Representatives from the relevant IC agencies meet to hone and coordinate line-by-line the full text of the NIE. Working with their agencies, representatives also assign the confidence levels to each key judgment.
- IC representatives discuss the quality of sources with intelligence collectors to ensure the draft

does not contain erroneous information.

- The National Intelligence Board, comprised of the directors of all 16 intelligence agencies, reviews and approves the document. The NIC then distributes the NIE to key policymakers in both the executive and legislative branches.

Challenges to the Production of NIEs

The IC must overcome several challenges to produce accurate and useful strategic intelligence assessments, including:

- *Urgent Requests vs. Lengthy Process*: The process of interagency coordination and an insistence on analytic rigor normally push the completion of NIEs to several months or even more than a year. Per Congress's request in the fall of 2002, the IC rushed to complete the NIE on Iraq's WMD programs in less than a month. Since a rushed product can result in poor or inaccurate assessments, the IC must balance the urgency for a requested assessment with a commitment to analytical rigor.
- *Interagency Collaboration*: Because NIEs represent the consensus view of the IC, all 16 agencies have input on each NIE. Such collaboration can lead to:
  - *Gridlock*, where many different interests slow the analytic process.
  - *Compromise*, where the estimates contain only "lowest common denominator" language.
  - *Groupthink*, where opposing views are subconsciously discouraged.

Politicization?

Throughout the past several decades, the release of a NIE on a controversial policy have usually resulted in charges that the IC politicized its key findings. Charges of politicization come from both Democrats and Republicans, but normally emerge from the side that does not agree with the policy implications of the analysis. Changes or reversals in NIE assessments over time cause some legislators to question whether the change resulted from newly collected intelligence or whether analysts changed their position to support a specific political agenda.

- For example, the IC accusation of politicization surfaced after the key judgments of NIEs on the ballistic missile threat to the United Sates changed between 1993 and 1995. Some Republicans claimed the IC politicized the findings to support President Clinton's policy against missile defense systems.
- Democrats accused the IC of politicization after the release of the NIE on Iraq's WMD programs because they believed they supported the policy decision to invade Iraq.

Congress has investigated the issue of politicization within the IC numerous times, as have

independent commissions. To date, these investigations have never found evidence of politicization by analysts.

Learning from the 2002 NIE on Iraq WMD

Beginning in June 2003, the Senate Select Committee on Intelligence (SSCI) conducted a formal review of prewar intelligence assessments on Iraq. Their report concluded:

- A groupthink dynamic led analysts, collectors and managers to interpret ambiguous evidence as conclusively indicative of a WMD program.
- Groupthink was so pervasive that formalized IC mechanisms established to challenge assumptions and groupthink were not utilized.
- In a few significant instances, the analysis in the Iraq NIE suffered from a "layering" effect whereby analysts based assessments on previous judgments without carrying forward the uncertainties of the underlying judgments.

Also in response to the problems with pre-Iraq war intelligence, the 2005 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (The Robb-Silberman Report) noted the need to:

- Collect more meaningful intelligence, especially Human Intelligence (HUMINT).
- Provide more rigorous analysis that avoids unwarranted assumptions and encourages diverse and independent perspectives.
- Include political/regional context in the analysis of technical issues.
- Emphasize long-term products instead of only focusing on short-term assignments.
- Train analysts and provide structure for learning the business and tradecraft of analysis.
- Actively question analysts on their assumptions.

The IC has already implemented several of these recommendations in its production of NIEs. Despite the controversy surrounding its key judgments, many consider the 2007 NIE on the Iranian nuclear program an indication of improvement because the IC:

- Based assessments on new intelligence, rather than relying exclusively on older information.
- Provided definitive indications of the level of confidence for key judgments.
- Avoided relying on conclusions of previous assessments and did not disregard the implications of new intelligence.

- Employed an outside group responsible for alternative analysis to test an alternative theory explaining the new intelligence and key judgments.
- Instead of "voting" on the NIE's key judgments to produce "consensus," the NIE included differing agency assessments within the body of the document rather than in the footnotes.

Future Issues

Policymakers should not consider NIEs to be conclusive or infallible predictions of the future. Estimates are precisely that: The IC's best informed estimate of a situation given available intelligence. Errors on the scale of the Iraq NIE have grave repercussions for the nation, so the NIE process must continue to improve to guard against similar failures.

Congress has an important role to play in ensuring that the IC continues to improve NIEs. Future issues surrounding NIEs will likely include some of the following themes:

- *Public Release*: An assessment of the value of declassifying and releasing NIEs to the public.
- *Politicization*: An examination of the time and methodological constraints facing the IC in producing NIEs, which may help manage expectations and combat perceptions of politicization.
- *The Fine Print*: A discussion that obliges policymakers to read important NIEs in their entirety—to read the fine print, per se—particularly when using intelligence to inform sensitive and politically contentious decisions.

Defense Intelligence

Largely due to its size, mission and capability, the Department of Defense (DoD) controls a significant portion of the nation's intelligence resources. As both a consumer and producer of intelligence, defense intelligence assets play a crucial and unique role in the Intelligence Community (IC).

This memo provides an overview of the structure of the nation's defense intelligence resources, defines the respective functions of defense intelligence, and highlights challenges to coordinating defense intelligence efforts with the rest of the IC.

What is Defense Intelligence?

Unlike the rest of the IC, DoD's intelligence capabilities primarily focus on providing units at all levels of the armed forces with the information necessary to successfully accomplish their respective missions. Some functions of defense intelligence include:

- Providing early threat warnings for deployed military forces.
- Supporting the decisions behind the technology acquisition process.
    - DoD uses evaluations of future threats to determine the appropriate investments in specific combat platforms and technologies.
- Informing commanders at the operational and strategic levels of military operations.
- Supplying critical tactical intelligence to smaller units and individual warfighters on the ground.

The DoD's intelligence assets are diverse and reflect a broad spectrum of military capabilities. Key components include:

- *Defense Intelligence Agency (DIA)*: A joint agency focused on intelligence collection and all-source analysis to support military customers and integrating products of military service intelligence activities and the Combatant Commands.
- *Military Service Intelligence*: Each branch of the armed forces has its own service intelligence center and intelligence organization. These units collect and analyze information to support that service's specific intelligence requirements while also contributing to larger IC information needs.
- *National Security Agency (NSA)*: This agency manages the nation's primary cryptologic and signals intelligence capabilities.

- *National Geospatial-Intelligence Agency (NGA)*: This agency administers the imaging and mapping of the Earth's surface.
- *National Reconnaissance Office (NRO)*: This agency oversees the design and operation of U.S. overhead reconnaissance systems.

Different Products for Different Customers

The IC serves two distinct customer sets—the President and senior civilian policymakers, and military commanders. While intelligence requirements for both sets of customers often overlap, each has information and programmatic requirements specific to its missions.

- This distinction is reflected in the congressional budgetary and oversight processes between the Military Intelligence Program (MIP), associated with defense intelligence, and the National Intelligence Program (NIP), which is essentially comprised of the rest of the IC.

The Need for Military Intelligence

When the National Security Act of 1947 created the CIA, a number of military intelligence organizations already existed. Because of perceived inadequacies in CIA's analysis of military matters, the armed services continued to provide intelligence support to the Pentagon and the Joint Chiefs of Staff.

- The Secretary of Defense and the Joint Chiefs of Staff insisted that DoD retain its own intelligence capability, because there were concerns that intelligence agencies outside the DoD could not provide flexible and sufficient support for the warfighter.
- DIA was created in 1961 to coordinate these various streams of intelligence, as well as coordinate information from across the armed forces.

During the debate over the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), senior defense intelligence officials testified to Congress that a non-DoD Director of National Intelligence (DNI) who completely controlled DoD intelligence assets might allow degraded support to defense and military requirements.

Because of the need for both civilian and DoD intelligence capabilities, some overlap naturally evolved within the IC, particularly in the areas of HUMINT and MASINT. Overlap in some areas promotes concentration of effort and alternative viewpoints; however, duplication of effort wastes resources, leads to clashes of jurisdiction, and may result in a sense of 'turf' that precludes information sharing.

The Under Secretary of Defense for Intelligence

The Under Secretary of Defense for Intelligence (USD(I)) provides oversight and policy guidance for DoD's intelligence activities under the joint authority of the Secretary of Defense (SECDEF) and the DNI. The USD(I) enables the DoD to accomplish its stated mission of supporting the "national, defense and international partners with 'knowledge-rich' all-source defense intelligence, counterintelligence, and security."

Because of the need for increased cooperation and mutual support in national security, the USD(I) also plays a significant role beyond the Defense Department as a leader in the greater IC.

- In 2007, the SECDEF and the DNI signed a memorandum of agreement that 'dual-hatted' the USD(I) as the Director of Defense Intelligence. Therefore the USD(I) now reports directly to the DNI as well as the SECDEF.
- Revisions of Executive Order 12333, the critical policy document that guides the organization and function of the IC, strengthened the relationship between the DNI and DoD and facilitated coordination between NIP and MIP resources. This new EO 12333 further integrated military and national intelligence activities and requirements.

In practice, the DNI sets national-level priorities—many of which draw on MIP programs, personnel, and assets—while the DoD retains direct tasking authority over its intelligence enterprise to meet the needs of the warfighter and the policymaker.

- This arrangement has not eliminated redundancies in the system. For example, CIA has military analysts and DIA has political analysts. These redundancies, however, can offer value in terms of competitive analysis and interagency cooperation.

Oversight Challenges

The recent changes in the IC's structure and the growing role of the DoD in combating terrorism abroad raises important oversight questions for members of Congress, including:

- *Extending the DNI-DoD "division" into Congress*. Splitting intelligence functions and resources into NIP/MIP categories effectively transferred some of the debate over national and military intelligence issues into the various oversight committees on the Hill. While the Senate and House Intelligence Committees both oversee the NIP, oversight responsibility for the MIP is shared in the House and mostly controlled by the Senate Armed Services Committee in the

Senate. This division of responsibility creates some uncertainty and tension about oversight roles of defense intelligence activities.

- *Oversight of "covert-action-like" defense intelligence activities.* Some clandestine defense intelligence activities may seem similar to covert action, but are not governed by reporting requirements established under the legal regime for covert action. Since Congressional notifications have not traditionally been required for clandestine actions authorized by military orders, DoD intelligence activities may receive less formal oversight than official covert actions or CIA clandestine activities.
- *Ensuring strong coordination between the DoD, the CIA, and the State Department.* Since 9/11, DoD has deployed military forces more frequently to non-combat environments and increased its clandestine collection to support military planning for future contingency operations. While these efforts are important and necessary, continued interagency coordination of defense intelligence activities overseas will be critical to avoid potential problems in national security operations and intelligence activities abroad.

Domestic Intelligence

Unlike many nations, the United States does not have a dedicated organization focused on domestic intelligence collection. Although the Federal Bureau of Investigation (FBI) is the principal domestic intelligence agency, the Central Intelligence Agency (CIA) and Department of Defense (DoD) also play limited domestic intelligence roles. In response to criticism following the attacks of 9/11, the FBI began reforms to increase their collection and analysis of domestic intelligence, especially in regards to terrorism. Nonetheless, critics contend that FBI intelligence collection continues to play a secondary role to the FBI's primary mission, federal law enforcement.

This memo provides new members of Congress with an overview of U.S. domestic intelligence and the issues most relevant to the 111th Congress.

Domestic Intelligence before September 11, 2001

Since its creation in 1908, the FBI has been responsible for both domestic intelligence and law enforcement. From the 1930s through 1960s, the FBI focused on cases of espionage and foreign subversion. The Church Committee investigation of intelligence abuses in the 1970s disclosed a series of FBI—along with CIA and NSA—violations of Americans' civil liberties. Congress passed a series of reform laws in the late 1970s, including the Foreign Intelligence Surveillance Act (FISA), to prevent future abuses.

In the wake of the intelligence scandals of the 1970s, concern about the potential for intelligence agencies to inappropriately collect information that could be used to prosecute citizens prevailed. This concern eventually morphed into a mistaken belief that intelligence officials could not legally share information with FBI criminal investigators. The resulting "wall" of bureaucratic obstacles virtually halted the flow of intelligence information provided to domestic law enforcement agencies. The 9/11 Commission highlighted this shortcoming as a major impediment to national security.

Post-9/11 Domestic Intelligence Paradigm

The attacks of 9/11 resulted in major organizational and functional changes within the Intelligence Community and dramatically shifted FBI priorities from traditional criminal matters to international counterterrorism threats and intelligence gathering.

After much debate, the 9/11 Commission recommended against creating a dedicated domestic intelligence agency, and instead recommended that the FBI expand and improve its intelligence

capabilities. In order to improve its domestic intelligence capacity, the FBI pursued the following initiatives:

- *Joint Terrorism Task Forces (JTTFs)*: The JTTFs are multi-agency task forces located in more than 100 locations nationwide. JTTFs bring local, state, and federal law enforcement and intelligence agencies together to share information and conduct operations to prevent terrorist operations. Prior to September 11, 2001, the United States had 35 JTTFs. Shortly after the attacks, the FBI Director instructed all FBI field offices to establish formal terrorism task forces.
- *Personnel*: The FBI hired hundreds of counterterrorism analysts and linguists, and re-tasked more than 700 personnel from criminal investigations to counterterrorism and counterintelligence duties.
- *National Security Branch*: The Bureau merged its intelligence, counterintelligence, and counterterrorism divisions into a unified "National Security Service" in 2005.
- *Field Intelligence Groups (FIGs)*: FIGs are composed of Special Agents, Intelligence Analysts, and other FBI specialists in each of the FBI's 56 field offices. They are designed to integrate the "intelligence cycle" into FBI field operations and manage the Field Office Intelligence Program in coordination with the Directorate of Intelligence at FBI Headquarters.
- *Domain Management Initiative*: In November 2005, the FBI launched the Domain Management Initiative to focus attention on national security threats within each field offices "geographic domain." The goal of program is to develop a comprehensive understanding of the threats relevant to each field office's region.

Assessing the Effectiveness of FBI Reforms

Opinions on Capitol Hill vary with respect to how successful the FBI has been in implementing their intelligence reform initiatives.

- Some indicate there is a critical synergy between law enforcement and intelligence—especially when addressing and thwarting terrorism threats. They believe the FBI's vision for intelligence reform is sound and that success is simply a matter of implementing that vision.
- Others believe law enforcement and intelligence are distinct disciplines that demand different skill sets. Ongoing FBI reforms have failed to produce an integrated intelligence program and that the FBI lacks the internal management acumen and vision to successfully transform itself into a premier domestic intelligence agency.

When the 9/11 Commissioners offered their final report on intelligence reform in December 2005, they gave the FBI a "C" and stated:

> "Progress is being made—but it is too slow. The FBI's shift to a counterterrorism posture is far from institutionalized, and significant deficiencies remain. Reforms are at risk from inertia and complacency; they must be accelerated, or they will fail. Unless there is improvement in a reasonable period of time, Congress will have to look at alternatives."

Institutional Changes Outside the FBI

Although the FBI is the lead agency for domestic intelligence, many other organizations within the government contribute to the collection, processing and analysis of domestic intelligence.

The Department of Homeland Security (DHS)

The Office of Intelligence and Analysis, located in the Department of Homeland Security, employs over 500 staff responsible for sifting through, analyzing, packaging, and disseminating intelligence based on information collected by DHS component agencies. I&A also integrates with the broader intelligence community and uses DHS links to state, local, and private sector partners to share information about potential threats.

The National Counterterrorism Center

Since 2005, FBI intelligence experts have been co-located at the National Counterterrorism Center (NCTC) with colleagues from across the Intelligence Community to assess and analyze terrorism threats.

Department of Defense

The Defense Department established the Counter Intelligence Field Activity (CIFA) in 2002 to counter threats to U.S. military installations and detect espionage against the Pentagon. CIFA had both intelligence and law enforcement functions. After a short and controversial existence in which several of its key programs were "disestablished", Secretary Gates merged CIFA into the Defense Counterintelligence and Human Intelligence Center at the Defense Intelligence Agency (DIA).

Outstanding Issues in Domestic Intelligence

Despite the reforms outlined above, improving the nation's domestic intelligence capability will remain an important issue for the 111th Congress.

Federal Bureau of Investigation (FBI)

As a lead domestic intelligence agency, the FBI continues to improve counterterrorism initiatives, intelligence sharing and capabilities. The 111th Congress will likely need to assess these and other reform issues that have expanded the mission of the FBI.

Department of Homeland Security (DHS)

As DHS continues to expand its intelligence activities, the Department has encountered potential hurdles to using intelligence assets to collect information within the United States. For example, DHS has proposed using overhead surveillance assets to provide domestic policymakers information about potential natural catastrophes, such as wildfires or hurricanes.

National Counterterrorism Center (NCTC)

Although the NCTC serves top policymakers, some experts assess that the NCTC does not push sufficient intelligence and information to state-level fusion centers, JTTFs, and local law enforcement.

Department of Defense

Some Members of Congress have expressed concern about DoD's increased role in domestic intelligence since September 11th. The 111th Congress will likely need to assess the value and legal authorities of DoD domestic intelligence assets.

Domestic Intelligence Developments

1910 | 1920 | 1930 | 1970

July 1908 1908

President Theodore Roosevelt authorizes the creation of the Bureau of Investigation—the precursor to the Federal Bureau of Investigation (FBI)—to manage interstate law enforcement.

1924-1972 1924-1972

J. Edgar Hoover, the first and longest-serving FBI Director, builds and strengthens the organization but faces criticism for employing heavy-handed tactics, including surveillance and harassment of domestic political activists.

1935 1935

The Bureau of Investigation is renamed the FBI.

July 1974 1974

The House Judiciary Committee issues articles of impeachment against President Richard Nixon, in part, for his authorization of illegal wiretaps against U.S. citizens.

1975-1976 1975-1976

A Senate Committee, headed by Senator Frank Church, investigates illegal activity on the part of the FBI and CIA, including the use of warrantless wiretaps against anti-war and civil rights leaders, forcing the FBI to scale-back domestic intelligence operations.

February 1993 1993

Islamic extremists detonate a car bomb below the World Trade Center in New York City, killing six people and injuring more than 1,000.

Domestic Intelligence

Developments

1980 1990 2000 2010

April 1995

Timothy McVeigh bombs the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, killing 168 people.

November 1997

Federal prosecutors convict Ramzi Yousef—the mastermind of the 1993 World Trade Center plot, who was captured in Pakistan in 1995—in New York of "seditious conspiracy" to bomb the towers.

September 2001

Nineteen al-Qaeda operatives attack New York City and Washington, DC using hijacked commercial airplanes, killing nearly 3,000 people.

February 2002

The Department of Defense creates the Counterintelligence Field Activity (CIFA) to manage the Department's counterintelligence efforts; CIFA was closed in 2008 following criticism of the agency's retention of files pertaining to domestic peace activists.

May 2003

The Terrorist Threat Integration Center, later renamed the National Counterterrorism Center, is formed as a clearing-house for analysis of domestic and foreign intelligence on terrorist threats to U.S. interests.

July 2004

The 9/11 Commission releases its public report, containing approximately 40 suggested reforms to the Intelligence Community and broader national security infrastructure, including measures to improve the flow of domestic and foreign intelligence.

December 2004

President George W. Bush signs the Intelligence Reform and Terrorism Prevention Act (IRTPA), which called for the creation of the Office of the Director of National Intelligence to ensure and manage the flow of domestic and foreign intelligence.

Intelligence and International Cooperation

Just as the Departments of Defense and State seek to develop strong alliances to achieve our military and diplomatic objectives, the Intelligence Community (IC) maintains robust 'liaison' relationships with many countries around the world. These relationships have proven important over the past several years, as other nations often have access to intelligence and can implement direct action that the U.S. requires to pursue its national security interests. While valuable, liaison relationships can also pose risks and require conscientious oversight by Congress.

This memo provides an overview of these foreign liaison relationships, as well as how these partnerships can strengthen U.S. national security.

Advantages to Foreign Intelligence Relationships

The U.S. benefits from international or liaison partnerships because they provide:

- *Access*: Liaison may have access to or information about areas denied to direct U.S. penetration.
- *Speed*: Liaison may be able to gather and disseminate crucial data, giving the U.S. the ability to respond to time-sensitive threats.
- *Insight*: Liaison may have greater cultural understanding into a particular issue that the U.S. may otherwise misinterpret.
- *Ability to Perform Direct Action*: Liaison sometimes can provide direct military force to solve a particular problem, usually within their home country.
- *Cover for U.S. Interests*: Liaison may be able to mask U.S. actions as local ones, obscuring otherwise obvious U.S. behavior in foreign countries.

Disadvantages of Foreign Intelligence Relationships

Liaison relationships with foreign services have disadvantages as well. The U.S. must remain vigilant for signs of:

- *Conflicting Interests*: Liaison may provide adversaries with critical sensitive information about U.S. interests, strategies and plans.
- *Hostile Collection*: Liaison may attempt to gain insight into U.S. intentions, sources and methods through overt or covert means.
- *Poor Information Gathering*: Liaison may use less rigorous collection methods than the U.S.,

often obliging Intelligence Community analysts to independently verify specific information.

- *Moral Hazards*: Members of foreign intelligence services may be involved in unethical or illegal activities, or utilize illegal methods to obtain intelligence.

International Cooperation

U.S. national security interests have long rested upon international cooperation between intelligence services. The post-WWII era ushered in a series of both formal and ad-hoc relationships that have linked the nation's various intelligence agencies, such as the Central Intelligence Agency (CIA) and the National Security Agency (NSA), with their foreign counterparts. Some examples of this cooperation include:

- Close cooperation between the U.S. and the United Kingdom in 2006 thwarted a plot to destroy civilian aircraft over the Atlantic Ocean.
- U.S. and Pakistan in 2003 worked in tandem to capture alleged 9/11 mastermind Khalid Shaykh Muhammad.
- The U.S. disseminates satellite imagery to third countries in order to combat narcotics production.

Commonwealth Partners

The U.S. maintains special intelligence relationships with the United Kingdom, Canada, Australia and New Zealand that generally allow for increased information sharing among the countries. This multilateral relationship, developed in the years after WWII, culminates in a high-level annual meeting that serves as a platform to discuss the various problems facing these nations.

Non-Traditional Allies

The U.S. also benefits from liaison relationships with organizations that are not nation-states. For example, the U.S. maintains partnerships with specific tribal groups and political parties, especially those that exist in countries that lack strong central governments but are nevertheless deemed critical to U.S. national security interests.

The U.S. has historically also worked with the security organizations in countries that provide unique links to key national security priorities. These relationships are often complex and require special oversight scrutiny from Congress. For example:

Pakistan: The U.S. relationship with Pakistan and its Inter-Services Intelligence (ISI) has arguably been one of the U.S.'s most complicated intelligence partnerships. The U.S. and Pakistan, along with Saudi Arabia, worked together to fund, train and equip Afghans fighting the Soviet Union in Afghanistan during the 1980s. Today, the ISI remains a critical and invaluable resource for the Intelligence Community to help locate Islamic militants, Taliban operatives and top members of al-Qaeda. Without assistance from the ISI, U.S. efforts to apprehend or eliminate major terrorist threats around the world would suffer significantly.

Some experts suspect, however, that small elements of the ISI and Pakistan's military establishment may be sympathetic to the Taliban and other militants. These suspicions have at times strained the U.S.-Pakistan security relationship. These conflicting signals compound pre-existing concerns by the U.S. about the ISI's general autonomy from Islamabad's command, as well as Pakistan's overall ability to maintain control over the increasingly chaotic Federally Administered Tribal Areas (FATA).

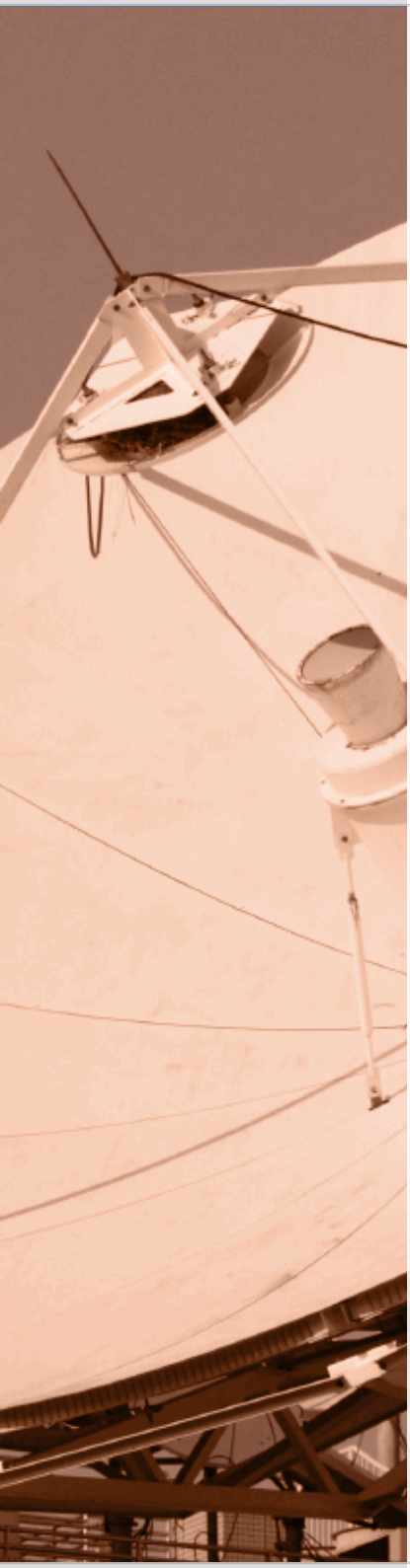
Sudan: While both countries can benefit from intelligence partnerships, especially when national interests align on the issue of counterterrorism, U.S. policymakers must decide if the benefits of a relationship outweigh concerns about the rule of law or human rights. For example, the U.S. and Sudanese intelligence officials worked together to track Usama bin Ladin when he resided in Khartoum during the 1990s. According to the press, Sudan has also occasionally assisted the U.S. in tracking al-Qaeda operatives. Nevertheless, the U.S.-Sudan relationship has been strained because of serious and legitimate concerns about the Sudanese government's involvement in the genocide in Darfur.

Considering Future Cooperation

As the IC continues to form new information-sharing relationships with foreign entities, members of Congress should continue to evaluate:

- *Motivations of Liaison Partners*: Foreign intelligence services are foremost concerned with their own self-interest, so the Intelligence Community and U.S. policymakers should remain cognizant that these organizations—even those considered friendly to the U.S.—may have ulterior motives in presenting information to American officials. Foreign liaison also may be motivated to exploit the U.S.'s significant capabilities to further their own interests.
- *The Scope of the Relationship*: The U.S. should consider the appropriate type of partnership that best suits each country's requirements. For instance, while some relationships may be based on short-term specific needs, others may encompass larger long-term strategies.

- *Potential for Broader Influence*: Liaison relationships between intelligence services can sometimes allow for warmer partnerships between the U.S. and potentially adversarial foreign entities. For example, the U.S. and China maintain a military-to-military relationship despite a sometimes contentious political history because the U.S. generally views the partnership as a mechanism to minimize miscalculations between the armed forces, foster pro-American feelings among younger Chinese officers and gain Chinese cooperation on specific international security issues.



Issue Memos

Intelligence Reform

The Intelligence Community's (IC) failure to prevent the 9/11 terrorist attacks and inaccuracies in the 2002 National Intelligence Estimate (NIE) on Iraq's weapons of mass destruction program resulted in widespread calls for reform. In late 2004, Congress passed intelligence reform legislation that led to the most significant reorganization of the IC in decades. More than four years after passage of the legislation, members of the 111th Congress will likely need to assess the effectiveness of the reform legislation.

This memo provides an overview of intelligence reform efforts since 2004.

The Need for Reform

Prior to 9/11, the nation's intelligence agencies remained poised for a single, traditional enemy and needed to adapt to a post-Cold-War threat environment. It was only after al-Qaeda attacked the U.S. that intelligence reform became a top priority for lawmakers. Several bipartisan and independent commissions reviewed the state of the IC and identified several areas for reform:

- *Central Leadership*: The Director of Central Intelligence (DCI) lacked the institutional or budgetary power to lead, direct, and coordinate efforts across the IC.
- *Information Sharing*: Bureaucratic structures and complex policies impeded, even prevented, sharing of important intelligence among the IC and other government agencies, particularly law-enforcement organizations. This highlighted the need for these communities to transform from a culture of "need-to-know" to one of a "responsibility-to-provide."
- *Priority Setting*: The IC did not sufficiently link and coordinate intelligence collection requirements to broader national security priorities.
- *Collection and Analysis*: Multiple investigations revealed weakness in the IC's human intelligence (HUMINT) collection efforts and cited the need for greater integration of analysis and collection disciplines.
- *Human Capital*: The number of people working in intelligence had atrophied since the Cold War. While well-positioned for an enemy like the Soviet Union, the profile of a generic intelligence analyst had not evolved culturally, demographically, or linguistically to target diverse threats in a new environment.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

The 9/11 attacks and concerns about the poor analysis of the Iraq WMD NIE created a sense of urgency for immediate, dramatic reform of the IC. In September 2004, Senator Susan Collins (R-ME) introduced the Intelligence Reform and Terrorism Prevention Act (IRTPA). The IRTPA initiated the most dramatic reform of the IC since its creation. Reform efforts initially met some resistance from some members of Congress.

- Some expressed concern that a national intelligence director with control of defense intelligence

assets could interfere in the chain of command between the Secretary of Defense and field commanders.

- Other members of the House Armed Services Committee opposed the IRTPA bill and sought to protect the authority of the Department of Defense over its national intelligence assets.
- The Bush administration, however, supported the legislation and pushed for compromises that protected the Pentagon's authorities while still creating the needed national intelligence authority to focus, guide, and coordinate the IC.

The IRTPA addressed many areas of reform, including organizational and leadership reforms.

Organizational and Leadership Reforms

In an effort to improve the organizational effectiveness of the IC, the IRTPA established:

- *The Office of the Director of National Intelligence (ODNI)*: The new cabinet-level DNI replaced the 'dual-hatted' Director of Central Intelligence as the independent leader of the nation's intelligence enterprise, designed to set policy and priorities, promote collaboration, and leverage the total capability of the IC to serve the nation.
- IRTPA established interagency centers, aligning analysis, collection, and operations from IC entities together under one roof to foster collaboration.
  - *The National Counterterrorism Center (NCTC)*: NCTC coordinates and integrates analysis of terrorism threats to the United States and its interests overseas.
  - *The National Counterproliferation Center (NCPC)*: NCPC coordinates the strategic planning of intelligence support to monitor and stop the spread of nuclear weapons and related technologies worldwide.

Information Sharing

Recognizing the value of information sharing to promote national security objectives, the ODNI created:

- *Information Sharing Environment (ISE)*: This partnership between all levels of the U.S. Government (including law enforcement), the private sector, and foreign allies, bridges the gap between foreign and domestic intelligence responsibilities and fosters sharing of timely and actionable terrorism information. Rather than creating a new information sharing system, ISE aligns and improves existing structures and facilitates integration through initiatives such as state and local fusion centers.
- *Collaborative Technology Tools*: ODNI continues to develop online applications to foster a culture of collaboration and improved information sharing. The use of classified encyclopedia-style webpages that any person with a clearance can modify (termed 'Intellipedia'), social networking sites like A-Space, and searchable databases such as the IC's Library of National Intelligence, capitalize on today's technology to encourage greater community collaboration and virtual integration.

Priority Setting

To organize and lead the IC into the post-9/11 threat environment, the ODNI initiated overarching efforts to identify, articulate, and align priorities for the IC, including:

- *National Intelligence Strategy of the United States of America (NIS)*: Based on the National Security Strategy, this document outlines objectives directed toward transforming the IC.
- *The 100 and 500 Day Plans for Integration and Collaboration*: These task-oriented documents serve as a roadmap for implementation of the NIS, focusing on initiatives such as transforming collection and analysis, implementing best business practices, and enhancing information sharing and collaboration.
- *Mission Managers*: These high-level intelligence executives serve as the manager of intelligence efforts focusing on key hard targets like Iran, North Korea and terrorism. The mission managers identify key information requirements and then design strategies to improve collection and analytic efforts to answer those requirements.

Human Capital

Per requirements levied in the intelligence reform legislation, the ODNI initiated several initiatives to improve and streamline the IC's use of human capital:

- *Quantity and Quality*: The 2006 ODNI Five Year Strategic Human Capital Plan outlined several initiatives to broaden the IC talent pool and compensate employees according to performance. This enterprise initiative was followed by the establishment of the National Intelligence Civilian Compensation Program.
- *Interagency Exchange*: To further collaboration and a culture of integrated enterprise in its workforce, ONDI created the Joint Duty Program. Mirrored after the Goldwater-Nichols concept of "jointness" in the military, the IC Joint Duty Program requires IC employees to complete a 12-month rotation in another agency as a prerequisite for promotion to senior ranks, demonstrating an emphasis on interagency cooperation in the IC's future leadership.
- *Security Clearance Improvement*: Because the process of obtaining security clearances was complicated and redundant, the IRTPA called for reciprocity between clearances at the same level and established entities to manage the clearance process and conduct clearance investigations. For example, the Joint Security Clearance Process Reform Team, an ODNI-DoD team, works to modernize the reciprocal security clearance recognition between the IC and the military.

Collection and Analysis

Some in the ODNI recognized the need to organize and make more efficient the collection and analysis process of the IC in the post-9/11 threat environment through:

- *HUMINT Collection*: To address the evolving and transnational nature of today's security environment, the IC is trying to upgrade its HUMINT capabilities.
- *Increased Integration of Collection and Analysis*: Linking collectors and analysts to further refine information requirements is an IC priority. Such closer collaboration fosters not only a greater sense of community and information sharing but also increases precision and clarity in analytic assessments for policymakers because analysts better understand limits in collection and information.
- *Alternative Analysis*: The 9/11 and WMD Commissions identified "devil's advocate" and alternative analyses processes to be essential to improving the IC's ability to critically analyze information and anticipate unexpected future threats and challenges for policymakers.

Nevertheless, the ODNI Inspector General in early 2009 publicly released a report faulting the ODNI for failing to achieve its longstanding goals of integrating the IC and sharing information. The report stated:

- "The majority of the ODNI and IC employees (including many senior officials)…were unable to articulate a clear understanding of the ODNI's mission, roles, and responsibilities with respect to the IC."
- The ODNI sends conflicting tasks and messages to the IC, "…thereby undermining the ODNI's credibility and fueling assertions that the ODNI is just an 'additional layer of bureaucracy.'"
- The ODNI staff's authorities are unclear, encouraging some agencies "…to go their own way, to the detriment of the unified and integrated intelligence enterprise envisioned by IRTPA." Compounding this issue is that IC computer systems are "largely disconnected and incompatible."

Issues for the 111th Congress

Challenges with the IC remain; in particular, Congress should assess:

- *Organizational and Leadership Reforms*: Some agencies resisted the creation of the ODNI because of concerns that it would infringe upon their roles and responsibilities and add another layer of bureaucracy.
- *Bureaucratic Bloat*: While most experts agree that a central leader dedicated to managing the whole of the IC is valuable, the ODNI may have grown too quickly and too large. Members of Congress should continue to review the size, structure, and effectiveness of ODNI.
- *Information Sharing*: While a marked improvement since 9/11, information sharing between law enforcement and foreign intelligence agencies remains a challenge. For example, a 2006 Government Accountability Office (GAO) report assessed the U.S. still lacks effective policies and processes for sharing counterterrorism information and cited inconsistent classification rules as an impediment to exchanging intelligence.

Intelligence Reform Initiatives

July 1947 1947

President Harry Truman signs the National Security Act, which reorganizes the Armed Forces and creates the CIA, among other reforms.

September 2001 2001

Nineteen al-Qaeda operatives attack New York City and Washington, DC using hijacked commercial airplanes, killing nearly 3,000 people.

May 2003 2003

The Terrorist Threat Integration Center (TTIC) is formed as a clearing-house for analysis of domestic and foreign intelligence on terrorist threats to U.S. interests.

1940 1950 1960 1970

December 1981 1981

President Ronald Reagan signs Executive Order 12333, which in part delineates the responsibilities of the Intelligence Community and places additional restrictions on the conduct of intelligence activities both domestically and abroad.

November 2002 2002

The Homeland Security Act creates the Department of Homeland Security to oversee the activities of 22 previously separate federal agencies.

July 2004 2004

The 9/11 Commission releases its public report, containing approximately 40 suggested reforms to the Intelligence Community and broader national security infrastructure.

Intelligence Reform In

August 2004 2004

President George W. Bush modifies Executive Order 12333, restructuring the Intelligence Community to 16 agencies, converting TTIC into the National Counterterrorism Center, and granting the Justice Department authority over most domestic intelligence activities.

April 2005 2005

John Negroponte, a career diplomat who previously served as U.S. Ambassador to Iraq, wins Senate confirmation and is sworn-in as the first Director of National Intelligence (DNI).

December 2005 2005

The National Counterproliferation Center (NCPC) is formed as an interagency body to track nuclear weapons and material, as mandated by the IRTPA.

1980 1990 2000 2010

December 2004 2004

President Bush signs the Intelligence Reform and Terrorism Prevention Act, which calls for a major overhaul of the Intelligence Community, including the creation of the Office of the Director of National Intelligence (ODNI).

October 2005 2005

The ODNI releases the National Intelligence Strategy of the United States of America, outlining a strategy to carryout the mandated Intelligence Community reforms.

July 2008 2008

President Bush signs Executive Order 13470 as an amendment to Executive Order 12333, bestowing more authority to the DNI by declaring him, for example, the overseer of relationships with foreign liaison services.

ITIATIVES

Interrogations and Intelligence

On January 22, 2009, President Obama issued an executive order mandating that all government agencies conducting interrogations follow the guidelines outlined in the U.S. Army Field Manual on Interrogation. Administration officials nevertheless left open the possibility that new, separate guidelines could be established in the future to govern interrogations conducted by intelligence agencies.

This memo provides new members of Congress with an overview of the guidelines for interrogations conducted by the military or intelligence agencies. This memo also provides a brief background on the debate about 'coercive interrogations' that transpired over the past several years.

Defining Interrogation

U.S. military intelligence doctrine states that interrogation is:

> "The systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning."

U.S. Army Field Manual 2 22.3 (FM 2-22.3) entitled "Human Intelligence Collector Operations," suggests that a successful interrogation produces needed information that is timely, complete, clear, and accurate.

- The goal of any interrogation is to obtain usable and reliable information, in a lawful manner and in the least amount of time, which meets intelligence requirements of any echelon of command.

The Detainee Treatment Act of 2005 and FM 2-22.3 provide "uniform standards" for interrogation, as well as prohibit "cruel, inhuman, or degrading treatment or punishment" of detainees, as interpreted through the United States Constitution.

- According to the U.S. Army/Marine Corps Counterinsurgency Field Manual, U.S. law "clearly prohibits U.S. forces, including officials from other government agencies, from using certain methods to obtain information." Nevertheless, the Detainee Treatment Act appears to only apply to individuals in Department of Defense (DoD) facilities, and not to other facilities maintained by other government agencies.
- In March 2008, President Bush vetoed a bill that would have compelled all U.S. interrogators—including individuals working for the Central Intelligence Agency (CIA)—to comply with the U.S. Army field manual on interrogations.

- On January 22, 2009, President Obama issued Executive Order 13491 which restricted the U.S. Government's interrogation methods to the measures dictated by the U.S. Army Field Manual.

Who May be Detained and Interrogated in Wartime?

Beyond uniformed enemy belligerents, and given U.S. commitments in counterterrorism and counterinsurgency operations in Iraq and Afghanistan, the types of detainees who may be interrogated in DoD facilities generally fall into two categories:

- Persons who have engaged in, or assisted those who engage in, terrorist or insurgent activities.
- Persons who have incidentally obtained knowledge regarding insurgent and terrorist activity, but who are not guilty of associating with such groups.

U.S. regulations and war doctrine assume that the Geneva Conventions apply to all aspects of detention and interrogation operations. Military personnel who engage in cruel or inhuman treatment of detainees during interrogation can be punished under the Uniform Code of Military Justice (UCMJ).

- Only people who are trained and certified to be interrogators may officially conduct interrogations. These interrogators use legal, approved methods of convincing detainees to give their cooperation.
- The interrogation manual stipulates that the "stated policy of the U.S. Army [is] that military operations will be conducted in accordance with the law of war obligations of the U.S."

A Brief History of U.S. Interrogation Programs since WWII

The U.S. has implemented several different interrogation programs during various conflicts with varying degrees of success.

- In the Pacific theater during the latter part of WWII, the U.S. Marines established an interrogation program based on establishing rapport with captured Japanese prisoners. This program proved so successful that the Marines in June 1944 were able to provide U.S. commanders with the complete Japanese order-of-battle within 48 hours of arriving on Saipan and Tinian.
- The CIA in 1960s and early 1980s published interrogation manuals that described various coercive techniques that might elicit information such as "threats and fear," "pain" and "debility." Some of these manuals were subsequently amended to state that certain practices were both illegal and immoral.
- In the current conflicts in Iraq and Afghanistan, tens of thousands of individuals have been interrogated without the use of coercive or harsh techniques.

The CIA Interrogation Program

Significant debate about interrogation policy emerged after revelations that the Bush Administration ordered and authorized the CIA to utilize "enhanced interrogation techniques" on high-value al-Qaeda detainees. In the weeks and months following the 9/11 attacks, political leaders and the Intelligence Community (IC) alike felt pressure to take steps necessary to prevent future—and possibly imminent—terrorist attacks. Thus, after being given permission by the White House and the Department of Justice, the CIA began using alternative interrogation techniques to gather intelligence from high-value al-Qaeda detainees. The subsequent disclosure of these techniques to the public, referred to as "coercive interrogation" or "enhanced interrogation techniques," fueled an ongoing debate over whether these interrogation techniques are effective, lawful and ethical.

It remains controversial whether coercive interrogation methods effectively elicit timely and accurate information from detainees. During a 2006 speech, President Bush claimed that enhanced interrogation techniques on a number of al-Qaeda members protected U.S. interests and gave interrogators information that stopped new attacks from reaching the operational stage.

- During the same speech, President Bush said these procedures were designed to "be safe, to comply with our laws, our Constitution, and our treaty obligations."
- The CIA director in 2007 claimed that interrogations of high-value detainees have been "historically the single greatest source of information we've had" on al-Qaeda.

Coercive techniques, however, may result in the U.S. obtaining faulty information, which in turn may lead to poor analytical outcomes and misinformed policy decisions.

- Experts still disagree whether Abu Zubaydah, one of the first al-Qaeda operatives caught after 9/11, provided critical information to U.S. interrogators through enhanced interrogation techniques. According to press reports from 2009 quoting senior U.S. officials, Abu Zubaydah provided the most useful information prior to being subjected to harsh measures, and no significant al-Qaeda plot was thwarted because of his debriefings.
- A Senate Intelligence Committee report found that Ibn Shaykh al-Libi, an al-Qaeda operative may have provided false or coerced information regarding a high-level relationship between al-Qaeda and Saddam Hussein prior to Operation Iraqi Freedom after he was detained and possibly aggressively interrogated by a third country.

The Obama Administration in April 2009 declassified another four subsequently-retracted memos from the Department of Justice that described, in detail, the legal justification for enhanced interrogation techniques.

- An August 2002 memo gave approval for specific coercive techniques, including waterboarding; since these techniques were not "specifically intended" to cause "severe physical or mental pain or suffering," the opinion stated they were indeed legal.
- Three May 2005 memos opined that waterboarding and other harsh techniques, whether individually or in concert, did not violate the federal criminal prohibition against torture since CIA had identified certain safeguards and limitations to the techniques. However, a footnote in one of the memos noted the CIA inspector general reported these rules were not always followed.

After releasing these controversial memos, the Obama Administration stated it was not interested in prosecuting current and former CIA officers who carried out coercive interrogations based on the Department of Justice's legal reasoning.

- President Obama however left open the possibility that the lawyers and policymakers who authored and authorized these opinions may face some civil or criminal penalties.
- Some Members of Congress as of May 2009 are planning to perform an independent public investigation into the CIA's coercive interrogation program.

Issues for the 111th Congress

As the 111th Congress debates the issue of enhanced interrogation, it will likely consider several factors, including:

- *The efficacy of coercive interrogation techniques*. Have coercive techniques provided the government with crucial, reliable information about actual threats? How many pieces of quality intelligence has the IC successfully generated from these techniques?
- *The costs and benefits of utilizing these techniques*. How does the intelligence gleaned weigh against the potential damage to the United States' international reputation? How significant is the threat that U.S. soldiers abroad face the risk of reciprocal treatment if captured by our enemies?
- *The feasibility of a single standard*. Should a U.S. Army Field Manual be the single standard for governance on interrogation methods for the U.S. intelligence community? Or should the IC have its own, possibly classified, standard?
- *The importance of secrecy*. Should interrogations guidelines for intelligence agencies be classified to deter foreign enemies from preparing resistance to these interrogation methods?

Interrogation Developments

1949 1949

The United Nations adopts the Third Geneva Convention governing the treatment of prisoners of war.

September 2001 2001

President George W. Bush in a sweeping Presidential Finding six days after 9/11 authorizes the CIA to kill, capture and detain al-Qaeda members globally.

August 2002 2002

The Justice Department's Office of Legal Counsel issues several opinions narrowly defining torture and discusses measures that could be used on high-value al-Qaeda detainees. These opinions are subsequently withdrawn as legally flawed.

1940 1950 1960 1970

1955 1955

The United States ratifies the Geneva Conventions.

March 2002 2002

U.S. and Pakistani authorities in Pakistan capture senior al-Qaeda lieutenant Abu Zubaydah and transfer him to the CIA's detention and interrogation program.

June 2004 2004

The existence of the Office of Legal Counsel's opinions on torture and interrogation techniques leaks to the media.

December 2004

The Justice Department issues a revised finding to the since withdrawn August 2002 memo, providing a broader definition of torture.

Interrogation Develop

November 2005

The Washington Post publicizes the existence of secret CIA detention centers, or "black sites," in several countries.

September 2006

President Bush confirms the existence of the CIA detention and interrogation program in a public speech, adding that 14 high-value detainees had been transferred to Guantanamo Bay, Cuba for prosecution.

February 2008

CIA Director Michael Hayden confirms during Congressional testimony that the CIA waterboarded three detainees—senior al-Qaeda lieutenant Abu Zubaydah, external operations chief Khalid Sheikh Mohammed and USS Cole mastermind Abd al-Rahim al-Nashiri—during the 2002-2003 period.

1980 1990 2000 2010

December 2005

Congress passes the Detainee Treatment Act of 2005, which requires the humane treatment of prisoners and restricts the U.S. military to the use of interrogation techniques approved by the U.S. Army Field Manual.

July 2007

President Bush signs Executive Order 13440, which prohibits the CIA from engaging in torture, as defined by the Detainee Treatment Act of 2005, and "willful and outrageous acts of personal abuse" done "beyond the bounds of human decency."

January 2009

President Obama issues an Executive order mandating all government agencies follow the U.S. Army Field Manual when conducting interrogations.

April 2009

The ACLU posts four previously classified Department of Justice memos detailing the use and extent of waterboarding by U.S. interrogators.

PMENTS

Electronic Surveillance and FISA

Electronic surveillance is one of the core methods the Intelligence Community (IC) utilizes to gather information on foreign adversaries and terrorist organizations. Public revelations that President Bush authorized the National Security Agency (NSA) to perform electronic surveillance on electronic communications with a domestic nexus, without a court-issued warrant, resulted in significant debate about the means, legality and effectiveness of electronic surveillance.

This memo provides an overview of electronic surveillance and discusses the recent debate in Congress about and the Foreign Intelligence Surveillance Act (FISA).

What is Electronic Surveillance?

Electronic surveillance refers to the acquisition of the contents of wire, radio and other electronic communications. Electronic surveillance has emerged as a critical tool for detecting and intercepting international terrorists within the United States and overseas.

Legal Basis for Electronic Surveillance

There are two main frameworks for electronic surveillance. One, based on Title III of the U.S. Code, covers surveillance in the investigation of serious domestic crimes. The second, based on FISA, covers foreign intelligence surveillance and serves as the main tool for electronic surveillance of international terrorists.

Congress passed FISA in 1978 in the wake of revelations that the White House authorized warrantless surveillance of Americans. In brief, the legislation stated:

- FISA would be the "exclusive means" governing the use of electronic surveillance in international terrorism and other foreign intelligence investigations.
- The Federal Bureau of Investigation (FBI) and NSA would serve as the lead agencies to gather foreign intelligence relevant to the FISA framework.
- The IC would work through the Foreign Intelligence Surveillance Court (FISC) to secure a warrant before undertaking foreign intelligence surveillance of a domestic nature.

Following 9/11, Congress and the White House agreed the IC needed greater flexibility to address the threat posed by international terrorism. Congress therefore passed amendments to the FISA legislation in the USA-PATRIOT Act in 2001. The USA-PATRIOT Act significantly eased the standard required of a federal officer to apply for intelligence collection under the FISA framework. Congress also adjusted and modernized FISA in the Protect America Act of 2007 and the FISA Amendments Act of 2008.

How FISA Works

Intelligence agencies do not need a warrant to collect information on foreign adversaries and terrorists with communications that occur outside the United States. When electronic communications either transit or occur within the United States, however, intelligence officials must use FISA. In sum, a *significant purpose* of the electronic surveillance must be to obtain intelligence in the U.S. on foreign powers (such as enemy agents or spies) or individuals connected to international terrorist groups.

- To use FISA, the government must show probable cause that the "target of the surveillance is a foreign power or agent of a foreign power."

Civil Liberties Protections

Under FISA, U.S. citizens, legal residents and U.S. corporations (known as "U.S. persons") are protected against illegal search and seizure by the Fourth Amendment; hence, FISA includes a number of provisions to protect civil liberties. Furthermore, FISA also explicitly states that, "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment of the Constitution of the United States."

While surveillance of U.S. persons is permitted under FISA, the IC must "minimize" the collection of information not directly applicable to the intended target.

- These strict minimization procedures require the IC to obscure the identity of any protected communications incidentally captured as part of the surveillance.
- Unlike Title III criminal warrants, however, minimization occurs after collection under FISA.

Controversy Regarding Electronic Surveillance

In December 2005, the *New York Times* revealed that President Bush authorized the NSA to conduct a warrantless surveillance program. The White House stated that the program targeted the international communications of individuals connected to al-Qaeda or other foreign terrorist organizations. Skeptics of the program feared that the President had overstepped the bounds of his authority and spied on Americans. The surveillance activities became known as either the "Terrorist Surveillance Program" (TSP) or "warrantless wiretapping."

As reports of the electronic surveillance efforts gradually became public, some argued the program was necessary to intercept al-Qaeda-related communications more quickly than the FISA process allowed. They claimed that the process for obtaining FISA warrants for each individual target prevented the government from obtaining this data in a timely fashion.

As questions about the legality of the surveillance program grew, proponents argued that:

- The President could legally ignore FISA because he possessed the inherent authority to conduct warrantless surveillance for intelligence purposes as part of his constitutional Article II powers as Commander in Chief.
- The Congressional Authorization for Use of Military Force (AUMF) of September 18, 2001 provided authority for the President to take these actions.

On the other hand, others argued the President could not completely bypass the FISA process because Congress explicitly intended FISA to be the "exclusive means" for authorizing this type of surveillance.

- This perspective indicated that the AUMF was not intended to cover electronic surveillance, particularly since Congress passed the USA-PATRIOT Act to amend various parts of FISA almost immediately after it passed the AUMF.
- Furthermore, some argued the program offered too few protections to prevent the government from monitoring the communications of innocent Americans and lacked appropriate congressional oversight.

In January 2007, Attorney General Alberto Gonzales informed Congress that the FISC had issued orders authorizing the collection of international communications into or out of the United States when the government had probable cause to believe that the communications belonged to a terrorist organization. Gonzales noted that because of the FISC order, the President would discontinue his authorization of TSP and conduct all electronic surveillance under FISA.

FISA Modernization

Although debate about the legality of the TSP continued, most members of Congress agreed that technological evolutions required "modernization" of the FISA legal framework.

One reason for updating the law was that the telecommunications industry had evolved significantly since the inception of FISA in 1978. Most importantly, a large portion of international communications moved from satellites, which are "radio" communications under FISA, to fiber-optic cables, which are "wire" communications under FISA. The original law did not regulate international radio communications unless the government targeted a U.S. person.

- FISA originally regulated international wire communications only when the surveillance was conducted in the U.S. Since a significant portion of the global fiber-optic network currently passes through the U.S., the government argued that FISA should be modified to allow for foreign intelligence surveillance of non-U.S. persons from within the country.

Nevertheless, there was concern that attempts to modernize FISA risked weakening civil liberties protections by removing the individualized warrant requirement that underpinned the original FISA law. Some believed that program warrants and longer periods of emergency warrantless surveillance could have further undermined the intent of original protections.

- Some argued the "communications revolution" argument was overblown. The shift of international communications that from satellites to fiber should not impact the FISA review process.
- Some also saw in FISA modernization a way to facilitate additional 'backdoor' intelligence gathering practices, such as large-scale data mining.

The FISA Amendments Act of 2008

While a number of FISA-related issues remain for Congress to resolve in the future, the FISA Amendments Act of 2008 (set to expire in 2012) addressed the following issues:

- FISA and Title III remain the *exclusive means* for conducting electronic surveillance.
- In order to conduct electronic surveillance of U.S. persons located outside the country, the government must now go through the FISA court order process; previously, the Attorney General could certify this collection under an executive order.
- A provision permits greater use of "program warrants" in order to target broad groups of foreign targets, as opposed to more individualized ones.
- The Attorney General has an extended period during which he can approve surveillance without a warrant in emergency situations.
- Congress granted telecommunications service providers immunity from prosecution for cooperating with government surveillance programs, as long as they received written government assurances about the legality of their cooperation from the government.
- Relevant Senate and House committees will receive from the Attorney General a semi-annual report on FISA-based targets.
- Congress included a number of added oversight and reporting requirements in order to play a more active role in reviewing the government's use of FISA.

Electronic Surveillance Developments

June 1934 1934

Congresses passes the Federal Communications Act, the first legislation regarding the use of wiretaps.

June 1968 1968

Congress passes the Omnibus Crime Control and Safe Streets Act, which includes the first federal legislation restricting the use of wiretaps in an effort to "safeguard the privacy of innocent persons."

1975 1975

A Senate Committee, headed by Senator Frank Church, investigates illegal activity on the part of the FBI and CIA, including the use of warrantless wiretaps against anti-war and civil rights leaders.

1940 1950 1960 1970

December 1967 1967

The Supreme Court extends Fourth Amendment protections in Katz v. United States, ruling that the government must obtain a warrant before initializing wiretaps and that warrants must be limited in scope and duration. The Court, however, allows for exceptions in cases involving national security.

July 1974 1974

The House Judiciary Committee issues articles of impeachment against President Richard Nixon in part for his authorization of illegal wiretaps against U.S. citizens.

October 1978 1978

Responding in part to the Watergate scandal and the Church Committee findings, Congress passes the Foreign Intelligence Surveillance Act (FISA) and creates the Foreign Intelligence Surveillance Court.

Electronic Surveillance

October 1986 1986

Congress passes the Electronic Communications Privacy Act to restrict electronic surveillance on new technologies, including computers, cell phones, and pagers.

December 2005 2005

The New York Times first reports on the NSA's "Terrorist Surveillance Program."

February 2008 2008

PAA expires under its sunset clause, requiring Congress to once again deliberate and construct an effective amendment to FISA.

1980 1990 2000 2010

October 2001 2001

President George W. Bush signs the USA-PATRIOT ACT into law, which among other measures streamlines the process of obtaining warrants to conduct surveillance and amends FISA to allow surveillance to cover people, rather than individual devices.

August 2007 2007

President Bush signs the Protect America Act of 2007, legalizing some forms of warrantless surveillance and to account for technological advancements since the passage of FISA in 1978.

July 2008 2008

Congress passes the FISA Amendments Act, which includes immunity for all telecommunication companies and eases restrictions on surveillance of targets outside the United States.

e Developments

Cyber Security and the Intelligence Community

The United States information infrastructure, ranging from telecommunications to computer networks, is the foundation for much of the business, military and civilian activity that occurs daily throughout the country. Over the years, these systems have become increasingly complex and interconnected, and the tools and methods to attack our core information architecture—including critical national security systems—have multiplied as well. Hence, U.S. policymakers ought to pay increased attention to protecting, defending and responding to attacks on information systems and networks.

This memo provides members new members of Congress with an overview of cyber security and the potential areas in which the Intelligence Community (IC) can support the nation's cyber security efforts.

The Cyber Threat

The significance and potential impact of cyber threats to the United States has grown quickly over the past decade. Cyber attacks can potentially undermine:

- Information systems and military responses.
- Civilian and military aviation systems.
- Critical first-response systems, especially during times of crisis.
- Financial markets and the free flow of financial data.
- Electric power grids.

The last several years have provided a number of examples for the potential damage that a coordinated cyber attack may wreak upon a nation's information infrastructure. These instances include:

- Russia-based hackers during the summer of 2008 assaulted the Republic of Georgia's government websites and commercial internet servers during the country's conflict with Russia.
- Russia-based hackers in May 2007 attempted with some success to undermine Estonia's Internet and banking systems through denial-of-service attacks during a politically tense period between the two countries. Russia has denied any official involvement in attacking Estonia.

The U.S. cyber infrastructure is susceptible to foreign and domestic attacks, and the breadth of our information architecture makes security breaches nearly inevitable. Unsurprisingly, the U.S. national

security system comes under special assault from malicious forces.

- The Department of Homeland Security (DHS) reported over 18,000 cyber-related incidents against federal agencies and more than 80,000 attacks on military computer systems in 2007.
- The Department of Defense (DoD) reported during a May 2008 House Intelligence Committee hearing that U.S. military systems are scanned or attacked more than 300 million times per day. Along these lines, China-based hackers probably penetrated U.S. military networks in 2007, according to DoD. Previously, some experts have alleged that China-based hackers allegedly penetrated unclassified military systems in 2001, nodes in the northeastern U.S. electric power systems in 2003 and computers in the U.S. Congress in 2008.

U.S. lawmakers are not immune from foreign cyber attacks on their personal and professional property.

- China-based hackers allegedly attacked computers in 2006 and 2007 used by a human rights subcommittee of the House Committee on Foreign Affairs, according to two Members of Congress. China's Foreign Ministry subsequently denied the charges.
- During a trip to Beijing in 2007, spyware programs were clandestinely placed on electronic devices used by the Secretary of Commerce and potentially other members of a top U.S. trade delegation.

Recent National Initiatives

In recent years, policymakers have recognized the importance of securing our information infrastructure and responded by increasing resources and focus on cyber security. These efforts have included:

- *The National Strategy to Secure Cyberspace of 2003*: Aimed at preventing cyber attacks against critical U.S. infrastructures, reducing national vulnerability, and minimizing the damage and recovery time from cyber attacks that do occur.
- *The "Einstein Program" of 2003-U.S. Computer Emergency Readiness Team (US-CERT)*: Created an automated process for gathering and sharing security information through DHS.
- *The Comprehensive National Cybersecurity Initiative of 2008 (CNCI)*: a classified "multi-agency, multi-year plan to secure the federal government's cyber networks."

The Intelligence Community: Bolstering U.S. Cyber Security

The IC takes a leading role in preventing cyber attacks and protecting the U.S. information infrastructure. According to press reports, various organizations within the IC could pursue some of the following tasks:

- *Office of the Director of National Intelligence (ODNI)*: Head a task force coordinating efforts to identify sources of future cyber attacks.
- *Department of Homeland Security (DHS)*: Lead for protecting government computer systems.
- *Department of Defense (DoD)*: Devise strategies for potential counterattack of cyber attackers.
- *National Security Agency (NSA)*: Monitor, detect, report and respond to cyber threats.
- *Federal Bureau of Investigation (FBI)*: Lead national efforts to investigate and prosecute cybercrimes.

Issues for the 111th Congress

The 111th Congress can support the IC by focusing on three particular aspects of preserving cyber security: organization, detection and deterrence.

National Organization: As the roles and responsibilities for the national cyber security effort evolve, Congress may consider whether the IC should play a leadership role on an issue that has significant policy and non-intelligence implications. For example, organizations such as the U.S. Strategic Command (STRATCOM), NSA and DHS could play an important role in managing overall cyber security efforts.

Early Detection and Warning: The IC should attempt to develop mechanisms of early detection in order to prevent attacks against our information infrastructure. The IC's leaders are aware of this threat—the Director of National Intelligence (DNI) in February 2008 stated that, "nations, including Russia and China, have the technical capabilities to target and disrupt elements of the U.S. information infrastructure…Terrorist groups—including al-Qaeda, Hamas and Hizballah—have expressed the desire to use cyber means to target the United States."

- The DHS Secretary in April 2008 announced that federal officials are trying to develop an early warning system that alerts authorities to incoming computer attacks targeting U.S. infrastructure.
- Any successful nationwide early warning system must be able to distinguish between small

cyber 'nuisances' and large-scale coordinated and targeted attacks that could significantly threaten the nation.

Deterrence: A comprehensive national deterrence strategy for cyber threats does not yet exist. Based on information gathered from previous attacks, the IC could begin to assess cyber threats through the lens of deterring future attacks.

- These assessments could provide policymakers with the foundation to craft a viable strategy to deter adversaries from attacking the nation's information architecture. A complete strategy will not only require awareness of possible threats, but also provides a credible response to attacks that would deter enemies from attacking in the first place.

Overhead Surveillance

One of the primary methods the U.S. uses to gather vital national security information is through air- and space-based platforms, collectively known as "overhead surveillance."

This memorandum provides an overview of overhead surveillance systems, the agencies involved in gathering and analyzing overhead surveillance, and the costs and benefits of this form of intelligence collection.

What is Overhead Surveillance?

"Overhead surveillance" describes a means to gather information about people and places from above the Earth's surface. These collection systems gather *imagery intelligence* (IMINT), *signals intelligence* (SIGINT) and *measurement and signature intelligence* (MASINT). Today, overhead surveillance includes:

- Space-based systems, such as satellites.
- Aerial collection platforms that range from large manned aircraft to small unmanned aerial vehicles (UAVs).

A Brief History of Overhead Surveillance

Intelligence, surveillance and reconnaissance platforms, collectively known as *ISR*, date back to the 1790s when the French military used observation balloons to oversee battlefields and gain tactical advantage over their adversaries. Almost all WWI and WWII belligerents used aerial surveillance to gain intelligence on enemy lines, fortifications and troop movements.

Following WWII, the U.S. further refined airborne and space-based reconnaissance platforms for use against the Soviet Union. Manned reconnaissance missions, however, were risky and could lead to potentially embarrassing outcomes; the 1960 U-2 incident was perhaps the most widely publicized case of the risks associated with this form of airborne surveillance.

Since the end of the Cold War, overhead surveillance technology has evolved significantly, greatly expanding the amount of information that the policymaker and the warfighter can use to make critical, time-sensitive decisions. For example, UAVs can remain over a target for hours or days providing pictures and full-motion video directly to the commander on the ground.

Overhead collection systems have been particularly useful in the Iraq and Afghanistan conflicts, as satellite and UAVs have allowed U.S. forces to identify adversaries and achieve greater accuracy in

striking targets.

- UAV use has increased at many levels, from "theater-level" systems to tactical systems flown by infantry battalions and even companies in combat.

Although overhead surveillance primarily supports military and counterterrorism operations abroad, overhead resources also have valuable domestic applications. For example:

- ISR systems have provided real-time support to fight wildfires in California.
- UAVs have been used to detect smugglers coming across U.S. borders.
- Satellites in 2005 provided imagery in Hurricane Katrina's aftermath, allowing assessments of the overall damage.

Which Agencies Control Overhead Surveillance?

Multiple organizations across the Intelligence Community control various overhead surveillance resources. The main organizations include:

National Reconnaissance Office

The National Reconnaissance Office (NRO) acquires, develops, manages and operates intelligence satellites. Established in 1961 as an agency within the Department of Defense (DoD), NRO's existence was officially denied until 1992. Although most of its programs and satellite capabilities remain classified, since 1995 NRO has declassified some systems from the 1960s and 1970s.

U.S. Air Force

The U.S. Air Force is responsible for aerial ISR. The USAF is increasingly reliant on UAV technology over manned reconnaissance vehicles because UAVs are cheaper to use and pose fewer risks for specific missions than manned aircraft.

National Geospatial-Intelligence Agency

The National Geospatial-Intelligence Agency (NGA) analyzes intelligence collected by NRO and Air Force assets. The NGA, previously known as the National Imagery and Mapping Agency (NIMA), then develops intelligence products from this information. The NGA is the principal producer of GEOINT, geospatial intelligence gained through the analysis of imagery and geospatial information. This information is used not only for military and policy purposes, but also for other uses such as disaster relief efforts.

Commercial Imagery Use

The Intelligence Community increasingly considers commercial imagery as a practical and less expensive alternative to using classified systems to obtain overhead data.

- Sharing commercial imagery with foreign governments and nongovernmental organizations sometimes allows the government to achieve policy and intelligence goals while still protecting sensitive classified imagery.
- Exploiting data from commercial imagery allows classified satellites to be reserved for sensitive missions.

In this vein, NGA frequently acquires commercial imagery to distribute to local, federal and non-governmental emergency management organizations.

- The NGA Director has publicly stated the Agency's desire to utilize commercial imagery as part of its future business plan, calling it "a fundamental building block" for the organization.

Implementation Challenges

Cost

The cost of overhead surveillance systems vary widely. Press reports estimate some overhead surveillance programs may cost billions of dollars. Recent evidence of the expense of these systems include:

- The Secretary of Defense in July 2007 shifted approximately $1 billion into ISR programs from other Pentagon accounts, citing the high priority of these systems.
- The Senate Appropriations Defense Subcommittee in September 2008 approved an additional $750 million in the 2009 defense appropriations bill for ISR efforts.

These costs are sometimes compounded by redundant systems found within the Intelligence Community. For example, the NRO and the Air Force frequently duplicate ISR efforts; as a result, several investigatory commissions have suggested integrating these programs.

- The most recent group to examine overhead surveillance systems, the Allard Commission, recommended changes to the way the U.S. manages overhead surveillance infrastructure.
- A related challenge to managing costs is that these systems are immensely complex, requiring a long lead time in developing not only the actual collection system, but also the processing and exploitation systems as well.

Domestic Surveillance Privacy Issues

The use of overhead surveillance by law enforcement or homeland security remains controversial, despite satellite imagery's utility in certain domestic assessments.

- Using satellites for homeland security and law enforcement purposes may infringe on privacy rights. It might also violate the Posse Comitatus Act that prohibits the use of military personnel and equipment for domestic purposes.

The Future

Overhead surveillance technology, in combination with overall intelligence gathering technologies, has improved drastically over the past decades. Given current national commitments in conflicts like Afghanistan and Iraq, expanding UAV technology will most likely be one of the short- and medium-term goals for the Intelligence Community.

- The small size and ease of use of UAVs have made these aircraft invaluable in tactical intelligence operations in Afghanistan and Iraq. Nevertheless, the Secretary of Defense stated that the technology is still being underutilized and should be expanded.
- The Allard Commission recommended that that the NRO be eliminated, and space-related authority that the Air Force currently possesses be transferred into a new National Security Space Authority (NSSA) to enhance the management of national security space operations.

The National Interest, Energy Security and the Intelligence Community

Over the past seven years, the Intelligence Community has focused its resources and attention on counterterrorism and support to ongoing military operations in Iraq and Afghanistan. Yet, volatile energy prices and the geopolitics of energy supply have rendered the United States more vulnerable than any time in past decades. Policymakers, including members of Congress, now recognize the need for the Intelligence Community (IC) to devote more attention to this important national interest.

This memo provides a proposed conceptual framework for assessing energy security and the potential areas in which the Intelligence Community can support policymakers.

What is Energy Security?

This paper takes a narrow, security-focused perspective on energy security. In that light, energy security is the "provision of affordable, reliable, diverse, and ample supplies of oil and gas… and adequate infrastructure to deliver these supplies to market."

Threats to Energy Security

Reliable energy inputs are crucial to U.S. national security.

- A sudden removal or disruption of energy inputs could adversely impact the U.S. economy and cause severe inflation.
- Rising fuel prices can bring windfall profits to regimes hostile to the U.S.
- Competition over scarce energy resources also has the potential to be a major source of conflict, which could directly impact supply or result in inter-state conflict.

Physical Threats to Energy Supply

Pipeline security: Most oil and natural gas pipelines run above-ground and extend over hundreds of miles, making them highly visible and difficult to protect. Pipelines are prime symbolic targets, seen as representing foreign influence and economic or political inequality.

- For example, politically motivated groups such as the Revolutionary Armed Forces of Colombia (FARC) and the Movement for the Emancipation of the Niger Delta (MEND) have attacked oil pipelines in Colombia and Nigeria, respectively.

Maritime Security: Oil and Liquified Natural Gas tankers are slow moving and rarely well-defended. Offshore platforms and ports are also vulnerable. In addition, global shipping lanes pass through narrow channels known as chokepoints, such as the Strait of Hormuz and the Bosporus Straits. An attack on, or interdiction of, a vessel in one of these chokepoints could result in closures or limits on traffic, which would seriously impact world energy supply.

- In November 2008, Somali-based pirates stunned national security experts by attacking and seizing a large oil tanker located more than 450 miles from the nearest coastline.
- Several terrorist groups, including al-Qaeda have threatened to attack oil tankers. In 2002, al-Qaeda was responsible for an attack on the *Limburg*, a French tanker.

Political Threats to Energy Supply

Control over the supply of energy is a major source of leverage for suppliers and transit countries.

- In January 2006, Russia cut off its supply of natural gas to Ukraine and threatened to do so again two years later. Many analysts asserted that Russia's actions were a politically motivated response to Ukraine's tilt towards the West.
- Both Iran and Venezuela have threatened to limit their oil production in the past year for political reasons.

The U.S. has sought to reduce the risk of such manipulation by supporting projects that involve U.S. allies, such as the Nabucco gas project in Central Asia, and opposing those that do not, such as the India-Pakistan-Iran gas pipeline.

World Energy Reserves

Energy suppliers do not always provide consistent or accurate information about their reserves. Yet policymakers and U.S. companies need this information to develop long-term energy policy and investments.

- Saudi Arabia, for example, often overstates or withholds its future production capabilities and plans. The rate of decline of the world's biggest oil field, Ghawar, as well the potential for the massive Khurais field, are both contested.

The Intelligence Community: Bolstering U.S. Energy Security

Addressing the challenge of energy security now and in the future will require the United States to utilize all instruments of national power, including using the IC. The IC could bolster support to policymakers and U.S. energy security in the following ways:

Strategic Look

The National Intelligence Council could complete a comprehensive National Intelligence Estimate on energy security that assesses the most vulnerable aspects of the infrastructure critical to delivering global energy supplies and the future stability of major energy suppliers.

Physical Threats

Pipeline Security: The IC is well-suited to gather information on the motivations and capabilities of groups who may attack targets crucial to the supply of oil and natural gas.

The ability of states to prevent and respond to attacks is also a fundamental aspect of energy security. Colombia, for example, found that a quick response by the government greatly reduced the effect of attacks on its energy. Intelligence officers could improve protection of facilities and contingency plans.

- The National Geospatial Intelligence Agency, for example, provided analysis of commercial imagery data on oil pipelines under construction and in operation in Russia and the Caucasus. The information was used to track the progress and security of the oil pipeline projects.
- Ideally, the government could work closely with the private sector to protect critical infrastructure.

Maritime Security: A GAO report in March 2007 critiqued the lack of information on the repercussions of an LNG tanker attack. The IC could provide such valuable analysis.

- The 2005 National Strategy for Maritime Security also noted the centrality of intelligence collection and analysis in maritime security. The Strategy described the importance of improving sensor technology and information processing tools, human intelligence and cooperation between domestic agencies and with our allies.

Political Threats

The IC could monitor decision-making circles in countries that have the power to impact U.S.

energy security. Collection targets could include oil ministries, traditional targets, such as the office of the head of state, or informal/private loci of power.

World Energy Reserves

To address our longer-term energy security, the IC could gather information on the status of the world's oil fields. This information would enable policymakers and experts to produce a timeline for developing alternatives and prepare for the possibility of unexpected energy shortages.

Terrorist Safehavens and the Intelligence Community

The attacks on September 11th highlighted that certain areas of the world without direct state control pose a direct threat to national security. These ungoverned areas—commonly referred to as safehavens—can provide terrorists and other adversaries with the space necessary to plot and train for attacks.

This memo provides new members of Congress with an overview of safehavens, as well as potential ways in which the Intelligence Community can support U.S. policymakers to mitigate the threat from these areas.

What are Safehavens?

The German political theorist Max Weber defined a nation-state as "a community that claims the monopoly of the legitimate use of physical force within a given territory." However, there are sections of certain countries that for one reason or another lie beyond the reach of that nation's security forces. These parts of the world remain ungoverned or under-governed, potentially allowing extremists to organize, plan, raise funds, communicate, recruit, train, and operate in relative security.

Ungoverned spaces have long challenged U.S. interests. Despite the efforts of the local security forces, areas nominally controlled by Lebanon, Algeria, and Colombia have sheltered extremist groups that have attacked U.S. interests in the past. Pakistan, Indonesia, the Philippines, and large swaths of Africa present similar challenges today.

- The World Bank has labeled 26 countries as "fragile" or fertile ground for terrorism, armed conflict, and epidemic disease.
- Small sections of otherwise stable states could also be added to this list: for instance, the "tri-border region" between Argentina, Paraguay and Brazil remains an area where extremist groups such as Hizballah operate relatively openly.

Case Study: Pakistan

A closer look at northwestern Pakistan in particular sheds light on the complexity of dealing with the safehavens.

Northwest Pakistan has been considered a safehaven for terrorists since December 2001, when the fall of the Taliban in Afghanistan pushed many of its members, along with members of al-Qaeda, across the border into Pakistan. Specifically, the Federally Administered Tribal Areas (FATA) in Pakistan—a politically chaotic area that mostly functions beyond the reach of Pakistani civil and military forces—have become the center of activity for al-Qaeda and other militants seeking not only to attack U.S. and coalition forces in Afghanistan, but also to launch operations in other countries as well.

- Most significant terror plots in Great Britain since 9/11 have had a Pakistan-based connection.

- Sovereignty concerns—and the perceived political fallout associated with violating Pakistani national borders—have prevented U.S. forces based in the region from mounting a systematic campaign to eradicate the extremist presence inside the FATA.

The Pakistan case also illustrates the predicament of relying upon local security services.

- Recent news reports suggest a growing body of evidence linking Pakistani intelligence to militant groups, some of which are responsible for attacks on U.S. interests in Afghanistan and elsewhere.
- Despite U.S. efforts to train and equip Pakistan's military to counteract the threat posed by extremists in the FATA, Pakistan has had little success in bringing the area under control.

The Intelligence Community's Role in Eliminating Safehavens

The U.S. Intelligence Community (IC) plays an important role in penetrating and denying safehavens to our adversaries in several ways:

Partnering with Liaison Services

The IC maintains liaison relationships with numerous other intelligence and security services around the world. In some cases, working with local services generates significant benefits for the U.S., as local services will have detailed knowledge, assets, and resources that the U.S. requires to pursue its national security interests.

- For example, the U.S. has worked with Pakistan's Inter-Services Intelligence Directorate (ISI) for many years—first against the Soviets during the 1980s in Afghanistan, and more recently against al-Qaeda. ISI's local knowledge of Pakistan and Afghanistan has proved invaluable and has led to the capture or killing of numerous al-Qaeda fighters within these and other safehavens.

Building Local Capacity

The IC has long worked with other countries' intelligence and security services to help make them more capable of monitoring and tracking terrorist activities within their borders. These efforts have led to several successful disruptions of terrorist attacks, such as in Jordan and Saudi Arabia. Such training programs can also help to ensure that governments can exercise legitimate control over their territories.

- For example, the Colombian government, with extensive U.S. cooperation, freed a group of hostages held by the leftist group Revolutionary Armed Forces of Columbia (FARC) in an ungoverned part of the country.

Establishing Persistent Surveillance of Ungoverned Spaces

Advances in Imagery, Surveillance, and Reconnaissance (ISR) platforms in the past decade have enabled the IC to monitor denied areas more effectively than in previous eras. Long loiter times and live video feeds—as well as the ability to identify, designate, and engage ground targets—allow unmanned aerial vehicles (UAVs) to monitor areas normally beyond U.S. and local government control.

The Role of Private Corporations in the Intelligence Community

Over the past several years, significant debate has emerged regarding the role that the private sector plays in national security operations. Since 9/11, the Intelligence Community has relied heavily on private contractors for many different types of support. Given the historic and growing ties between the Intelligence Community and private corporations, the 111th Congress will likely need to assess the overall value of this relationship.

This memo provides members of Congress and their staffs with an overview of the role of private corporations working with and within the U.S. Intelligence Community (IC).

The Intelligence Community and the Private Sector

The IC maintains relationships with private corporations to help meet national security goals. Reasons for this partnership include:

Technical Strengths

Private firms with specialized technical capabilities can be used to address to national security issues. Historically, government agencies such as the Central Intelligence Agency (CIA) and the Department of Defense (DoD) have worked with for-profit firms on various technical projects, such as:

- The U-2 spy plane—first used to conduct flights over the Soviet Union and still in operation today—was built through the CIA's collaboration with a private aeronautics firm.
- The MQ-1 Predator Unmanned Aerial Vehicle (UAV) was designed and built by a private firm for the U.S. Air Force.

Manpower and Managerial Expertise

Employees of private firms often have cultural, military, or linguistic backgrounds that are useful to the U.S. Government.

- *Protection*: Private firms guard buildings, personnel and U.S. infrastructure in diplomatic and military facilities throughout the world. For example, a private firm protects the U.S. Ambassador to Iraq and other key diplomats within the country.
- *Translation*: Contractors often serve as interpreters in U.S. detention facilities abroad.
- *IT Skills*: Private firms help with interagency coordination by providing collaboration tools across agencies, and they provide security tools for government computer systems.
- *Consultation*: Private companies provide strategy consulting services on various topics to the IC.

Workplace Flexibility

Government managers often employ contractors to quickly fill billets that otherwise might not suit permanent government positions. Contractors usually can also be removed from their positions with greater ease than government employees.

- After 9/11, the IC hired contractors to fill immediate staffing needs due to a shortage of available intelligence professionals; the former White House Coordinator for Security and Counterterrorism, however, suggests that the current contractor staffing levels stem from a lack of a long-term strategic plan by the IC for hiring and retaining personnel.
- Private firms supply manpower to fulfill the IC's mundane but critical functions, such as entering data into databases and other administrative obligations.

Contracting Controversies

The growing corporate presence within the IC has been controversial, as some would argue that contractors increasingly outnumber government employees in IC workspaces. The primary concern relating to this growth is that private contract employees may have started to complete tasks that were previous inherently governmental functions, such as intelligence collection or analysis. Some critics note that contractors maintain a fiduciary duty to their employer, not to the United States government.

Number of Contractors:

- According to some press reports, 51% of Defense Intelligence Agency's (DIA) staff currently are contractors.
- As of 2007, the DIA was preparing to pay private firms up to $1 billion to conduct "core intelligence tasks of analysis and collection" over the next several years, according to a press report.

Funding of Contractors:

- A presentation prepared in May 2007 by an Office of the Director of National Intelligence (ODNI) Senior Procurement Executive suggested that contracts with private firms make up approximately 70% of the IC's budget. The DNI later refuted these figures, stating that they were based on a "small, anecdotal sample of a portion of Intelligence Community contracting services."
- A Senate intelligence report conducted in May 2007 found that a contractor generally costs twice as much as a government employee; a federal worker costs approximately $126,500 while a contractor annually costs $250,000.

Governability of Contractors:

- Laws and regulations that define contractor behavior in conflict zones remain vague.
  - Many private employees fulfill military functions that distinguish them from civilians, yet they are not legally soldiers.
  - A 2004 Army investigation into detainee mistreatment in Iraq noted, "No doctrine exists to guide interrogators and their intelligence leaders…in the contract management or command and control of contractors in a wartime environment."
- When contractors engage in questionable behavior overseas, it remains unclear who is responsible for investigating, prosecuting, and punishing them.

The Future of Contracting?

The IC will rely heavily on private firms for intelligence functions in the future. Policymakers should therefore continue to refine the appropriate balance between internally and externally sourced tasks and responsibilities. Lawmakers should consider:

- What are the most effective means of accountability and transparency for contractors? How can Congress most effectively provide mechanisms for oversight, management, and evaluation of outsourced intelligence functions?
- What type of guidelines determine when is it appropriate for private firms to engage in sensitive intelligence functions, such as collecting intelligence, conducting covert action, and drafting finished analysis?
- When should private firms participate in necessary wartime functions, such as detaining and interrogating detainees?

The USA-PATRIOT Act

The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" also known as the USA-PATRIOT Act, was passed a month after September 11, 2001 in order to give U.S. officials new legal tools to detect and thwart future terrorist attacks. Although it originally passed with very little opposition, votes to reauthorize the Act prompted significant debate about several provisions. In 2009, Congress will once again examine certain sections of the USA-PATRIOT Act.

This memo provides an overview of the USA-PATRIOT Act and its provisions that will expire at the end of 2009.

Overview

Major provisions of the 2001 USA-PATRIOT Act included:

- Enhanced surveillance procedures for law enforcement, including amendments to the Foreign Intelligence Surveillance Act (FISA). Specifically, the Patriot Act gave federal officials new surveillance authority in terrorism cases, as well as the ability to conduct searches of property without the consent or knowledge of the owner or occupant.
- Increased federal authority to freeze financial assets of suspected terror groups and individuals.
- Measures enhancing border security, restricting suspected terrorist ability to obtain visas, and detaining suspected terrorists within the U.S.
- New criminal statutes broadening the category of terrorism-related offenses. In particular, the Act made it illegal to provide "material support" for terrorist activities.

Amendments to the PATRIOT Act Set to Sunset in 2009

The Act and subsequent reauthorizations included a number of temporary provisions that expanded federal authority to undertake surveillance in terrorism cases. Two provisions—one authorizing federal officials to use "roving" wiretaps and another giving federal officials the power to compel third parties to divulge business records—are set to expire at the end of 2009.

- Another controversial provision, dedicated to thwarting the so-called "lone wolf" terrorist, was part of the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA). This provision will also sunset in 2009.

The "Roving" Surveillance Provision

Section 206 of the PATRIOT Act allows investigators to track individuals with the same FISA warrant even if the suspect frequently changes his communication devices. Federal officers can now use the same warrant instead of obtaining a separate warrant for each phone, email address, apartment, or other facility used by the suspect.

- This authority was used 49 times between October 2001 and March 2005.
- The use of roving warrants is reported to Congress on a semiannual basis, and each specific order is reviewed by the Foreign Intelligence Surveillance Court (FISC).

In order to obtain a roving warrant, the federal agency must provide:

- A specific description of the target and the facilities or places the agency wants to monitor.
- Probable cause that the target is a foreign power (such as a foreign spy) or an agent of a foreign power, including members of a foreign terrorist organization.
- Information that indicates roving surveillance is necessary because the target might otherwise thwart normal surveillance procedures.

This provision addressed the likelihood that terror suspects change communication methods in order to evade detection.

- Without this 'roving' surveillance, investigators would have return to the FISC for every new phone that the suspect might use, allowing the suspect to evade detection.
- Similar roving surveillance had been successfully used by law enforcement in drug and racketeering investigations.

The 'Business and Other Tangible Records' Provision

Section 215 of the Act revised the rules governing federal officials ability to acquire business and other tangible records. 'Tangible records' include: business records, phone provider records, apartment rental records, driver's license records, library records, book sale records, gun sale records, tax return records, educational records, and medical records.

- Under this provision, federal investigators can compel third-party record holders, such as telecom firms, banks or others, to disclose these documents.
- Between October 2001 and March 2005, this provision was used 35 times to obtain credit card information, apartment leasing records, and telephone subscriber information on various individuals.

In order to use this provision, the U.S. must show that there are reasonable grounds to believe that the records are relevant to an international terrorism or counterintelligence investigation.

- The FBI Director or the FBI Deputy Director must personally approve applications for orders involving library, book sales, firearms, tax, educational or medical records.
- Recipients of an order can consult with legal counsel and challenge the order.
- The use of these orders must be reported to Congress on an annual basis.

Section 215's supporters suggest the orders are similar to grand jury subpoenas, but carry even more safeguards since they are approved by the FISA court.

- The "relevancy" standard for the records, along with heightened protections for library, book sales, gun sales, and medical records, protects privacy and First Amendment rights.

Critics of Section 215 argue that the "relevancy" standard can be used to obtain almost anything and that Congress should require a higher standard for law enforcement. Some believe heightened protections for library and other records may not be strict enough to protect privacy and First Amendment rights.

- Furthermore, some believe federal officials should not be allowed to obtain gun sales and library records in the first place.

The "Lone Wolf" FISA Provision

Section 6001 of IRTPA broadened FISA's scope by allowing surveillance of any non-U.S. person who engages or prepares to engage in international terrorism. A "lone wolf" refers to an individual who commits terrorist acts but lacks an explicit connection to a foreign power or a terrorist organization.

- Ordinarily, FISA allows surveillance only if the target is a foreign power—for instance, a country or a terrorist group—or an agent of a foreign power. Thus, in order to conduct surveillance of a "lone wolf," investigators would be obliged to show that the suspect meets the definition and all other FISA requirements.
- While not part of the original USA-PATRIOT Act, the 2006 Patriot Act mandated the "lone wolf" amendment to expire at the same time as Sections 206 and 215; hence, U.S. lawmakers will probably debate these provisions at the same time.

The "lone wolf" amendment may close a critical gap in FISA law by ensuring that all individuals

engaged in terrorist activity can be targeted.

- Investigators would be able to target international terrorists irrespective of whether a wider network has been identified.
- Moreover, by requiring probable cause to indicate the target is engaging or preparing to engage in a terrorist act, supporters argue that the "lone wolf" amendment has sufficient safeguards to prevent targeting unrelated persons.

On the other hand, by eliminating the requirement of some connection to a foreign power or an agent of a foreign power, the "lone wolf" provision may allow federal authorities to cast a wide net over many people, including individuals with little connection to terrorism.

State and Local Fusion Centers

The 9/11 Commission Report emphasized the importance of information sharing between local law enforcement and federal intelligence agencies in order to prevent future terrorist attacks. In an effort to address these concerns, "fusion centers" were created that would facilitate the transfer of information among local, state and federal officials.

This memo provides members of Congress with an overview of fusion centers, explains the role these centers play in information sharing and addresses some challenges that they face today.

What are Fusion Centers?

The Department of Justice (DOJ) defines a fusion center as a:

> …Collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

Centers may include federal, state, and local law enforcement representatives, as well as federal intelligence officers.

- As of February 2009, 58 fusion centers operated nationwide, 43 of which were fully functioning and 15 were still under development. In at least 34 of these centers, federal officers from intelligence and law enforcement agencies collaborate with their local-level counterparts.
- Many fusion centers are now expanding beyond counterterrorism efforts to serve as "all-hazards" centers that address criminal and emergency response needs.

Importance of Information Sharing

Fusion centers may be useful conduits for information, as state and local law enforcement officers are often the last line of defense against terrorist activity and attacks:

- Timothy McVeigh was arrested for the bombing of the Alfred P. Murrah Federal Building when an Oklahoma state trooper pulled him over for driving a vehicle without a license plate.
- The so-called Olympic Park Bomber, Eric Robert Rudolph, was only apprehended after a local police officer in North Carolina arrested him on an unrelated charge.

- *Missed opportunity*: Ziad Jarrah, one of the 9/11 hijackers, was pulled over by a Maryland state trooper two days before the attacks. The trooper was unable to identify the CIA-watchlisted Jarrah because he and the FBI did not have access to the CIA list.

Relationship to the Federal Government

Fusion centers are entities run by state and local governments. However, the federal government provides funding and expertise to these centers, largely through the Department of Homeland Security's (DHS) State Homeland Security Grant Program (SHSGP) and Urban Area Security Initiative (UASI).

- Federal funding requirements often require that fusion centers have dual reporting relationships to both state and federal officials.

In order to create basic standards across fusion centers nationwide, DHS and DOJ crafted the Fusion Center Guidelines (FCG). The voluntary guidelines were developed to help define the centers' relationship with the federal government as well as to protect civil liberties.

- To encourage fusion centers to adopt the FCG, the federal government offers additional funding to those centers that adopt them. So far however, only 16 of the 58 fusion centers have received this additional federal funding.

Challenges Facing Fusion Centers

Fusion centers face several challenges including sustained funding, privacy concerns and information sharing issues.

Funding Concerns

- DHS does not guarantee consistent funding streams to fusion centers, calling into question each center's long-term viability. Centers unable to find alternative means of funding if they lose DHS grant money may be unable to continue operating or be only able to fulfill part of its mission.
- Some argue that federal funding should only be used for fighting terrorism, and not for other purposes such as local crime prevention and disaster relief.

Privacy Issues

The 9/11 Commission stated information sharing with local enforcement is vital for national security, but balance must be maintained to ensure this information does not violate federal civil liberty protections.

- Collecting information on U.S. citizens who have not committed a crime may violate the Federal Privacy Act of 1974.

Information Sharing Issues

Additional problems with fusion centers include:

- *Information dissemination*: Accessing federal networks and information databases often proves difficult to center employees, as information is often available only to federal employees and not all private sector, state and local fusion center employees.
  - DHS recognizes this problem and is currently working to provide access to classified data networks and portals for terrorist-related threat information to all fusion center staff.
- *Clearance issues*: Fusion center personnel receive security clearances from DHS and DOJ, but sometimes clearance issues preclude certain individuals from accessing specific compartmentalized data. Furthermore, over-classification of data complicates information sharing.
- *Standard Operating Procedures*: Though guidelines exist, no standardized procedures for all centers guide the type of information is collected, the methods utilized for collection, the manner in which it is analyzed or the form which it is reported.

Issues for the 111th Congress

With more than 50 fusion centers nationwide, Congress should consider several factors for the future:

- How fusion centers should be defined, including how they figure into the larger intelligence and law enforcement communities.
- Identifying metrics for gauging the efficacy, relevancy and impact of fusion centers on local, state and federal partners.
- Defining requirements for centers, and level of compulsion for these requirements.

- Sustaining fusion centers financially, including determining the level of federal funding and support for each center.
- Preventing infringements on civil liberties while enhancing overall national security through information sharing and analysis.

Sources

Intelligence Basics

Bruno, Greg and Sharon Otterman, "National Intelligence Estimates." Council on Foreign Relations. 14 May 2008. 19 March 2009 <http://www.cfr.org/publication/7758/national_intelligence_estimates.html>.

Central Intelligence Agency. 2009. Central Intelligence Agency. 19 March 12009 <https://www.cia.gov/offices-of-cia/clandestine-service/index.html>.

Defense Intelligence Agency. 2009. Defense Intelligence Agency. 19 March 2009 <http://www.dia.mil>.

"Establishment of the DNI Open Source Center Press Release. CIA Official Home Page. 8 November 2005. Central Intelligence Agency. Web. 19 March 2009 <https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr11082005.html>.

Henley-Putnam University: Intelligence, Counterterrorism, Protection. 2008. Henley-Putnam University. 19 March 2009 <http://www.henley-putnam.edu/518-233.htm>.

Lowenthal, Mark. Intelligence: From Secrets to Policy. 4th ed. Washington, D.C.: CQ Press, 2009.

National Reconnaissance Office. March 2009. National Reconnaissance Office. 19 March 2009 <http://www.nro.gov/index.html>.

National Geospatial-Intelligence Agency. 2009. National Geospatial-Intelligence Agency. 19 March 2009 <http://www.nga.mil>.

National Intelligence Council Mission. March 17, 2009. National Intelligence Council. 19 March 2009 <http://www.dni.gov/nic/NIC_home.html>.

"National Security Act of 1947." (Pub. L. No. 235, 80 Cong., 61 Stat. 496).

Office of the National Counterintelligence Executive. 2009. Office of the Director of National Intelligence. 19 March 2009 <http://www.ncix.gov>.

National Security Agency, Central Security Service. 2008. National Security Agency. 19 March 2009 <http://www.nsa.gov>.

Office of the Director of National Intelligence. 2009. Office of the Director of National Intelligence. 19 March 2009 <http://www.dni.gov>.

U.S. Department of Defense. 2009. U.S. Department of Defense. 19 March 2009 <http://www.defenselink.mil>.

U.S. Department of State. 2009. U.S. Department of State. 19 March 2009 <http://www.state.gov>.

United States Cong. Senate. Select Committee on Intelligence. General Michael V. Hayden, Director, Central Intelligence Agency Statement for the Record. 11 Jan. 2007. 19 March 2009 <https://www.cia.gov/news-information/speeches-testimony/2007/statement_011107.htm>.

United States Intelligence Community. 2009. United States Intelligence Community. 19 March 2009 <http://www.intelligence.gov/index.shtml>.

Weiner, Tim. Legacy of Ashes: The History of the CIA. New York: Doubleday, 2007.

Organization of the Intelligence Community

Central Intelligence Agency. 2009 Central Intelligence Agency. 19 March 2009 <https://www.cia.gov>.

Defense Intelligence Agency. 2009. Defense Intelligence Agency. 19 March 2009 <http://www.dia.mil>.

Defense Intelligence Agency. 2009. Defense Intelligence Agency. 19 March 2009 <http://www.dia.mil>.

F.B.I. Directorate of Intelligence. 2009 Federal Bureau of Investigation. 19 March 2009 <http://www.fbi.gov/intelligence/intell.htm>.

Information Sharing and Analysis. 2009. U.S. Department of Homeland Security. 19 March 2009 <http://www.dhs.gov/xinfoshare/>.

The Intelligence Reform and Terrorism Prevention Act (IRTPA). S. 2845. 19 March 2009 <http://thomas.loc.gov/cgi-bin/query/z?c108:S.2845:>.

Lowenthal, Mark. Intelligence: From Secrets to Policy, 2nd Edition. CQ Press: Washington DC, 2003.

National Counterterrorism Center. 2009. National Counterterrorism Center. 19 March 2009 <http://www.nctc.gov>.

National Geospatial-Intelligence Agency. 2009. National Geospatial-Intelligence Agency. 19 March 2009 <http://www.nga.mil>.

National Intelligence Council. 2009. National Intelligence Council. 19 March 2009 <http://www.dni.gov/nic/NIC_home.html>.

National Reconnaissance Office. 2009. National Reconnaissance Office. 19 March 2009 <http://www.nro.gov/index.html>.

National Security Agency, Central Security Service. 2008. National Security Agency. 19 March 2009 <http://www.nsa.gov>.

Office of the Director of National Intelligence. 2009. Office of the Director of National Intelligence. 19 March 2009 <http://www.dni.gov>.

Office of Terrorism and Financial Intelligence. 2009. U.S. Department of the Treasury. 19 March 2009 <http://www.treas.gov/offices/enforcement>.

ODNI News Release No. 9-05. 21 December 2005. Office of the Director of National Intelligence News Release. 19 March 2009 <http://www.fas.org/irp/news/2005/12/dni122105.pdf>.

Office of the National Counterintelligence Executive. 2009. Office of the National Counterintelligence Executive. 19 March 2009 <http://www.ncix.gov>.

Turner, Stansfield. Burn Before Reading: Presidents, CIA Directors, and Secret Intelligence. New York: Hyperion, 2005.

U.S. Department of Energy. 2009. U.S. Department of Energy. 19 March 2009 <http://www.energy.gov>.

U.S. Department of Justice. 2009. U.S. Department of Justice. 19 March 2009 <http://www.usdoj.gov>.

U.S. Department of State Bureau of Intelligence and Research. U.S. Department of State. 19 March 2009 <http://www.state.gov/s/inr>.

U.S. Drug Enforcement Administration. 2009. U.S. Drug Enforcement Administration. 19 March 2009 <http://www.usdoj.gov/dea>.

United States Intelligence Community. 2009. United States Intelligence Community. 19 March 2009 <http://www.intelligence.gov/index.shtml>.

Congressional Oversight of the Intelligence Community

Best, Richard A. Jr. "Proposals for Intelligence Reorganization 1949-2004" (CRS Report for Congress RL32500). 24 September 2004. Foreign Affairs, Defense, and Trade Division, Library of Congress. 19 March 2009 <http://www.fas.org/irp/crs/RL32500.pdf>.

Kaiser, Frederick M., "Congressional Oversight of Intelligence: Current Structure and Alternatives " (CRS Report for Congress RL32525). 16 September 2008. Government and Finance Division, Library of Congress. 19 March 2009 <http://www.fas.org/sgp/crs/intel/RL32525.pdf>.

National Commission on Terrorist Attacks. (2004). The 9/11 commission report: Final report of the National Commission on Terrorist Attacks upon the United States. New York: W.W. Norton.

Pincus, Walter. "House Nears Passage of Resolution To Add Intelligence Oversight Panel." Washington Post 9 January 2007: A04.

U.S. Government Accountability Office. 2009. U.S. Government Accountability Office. 19 March 2009 <http://www.gao.gov>.

The Congressional Authorization and Appropriation Processes

Office of Management and Budget. 2009. Office of Management and Budget. 19 March 2009 <http://www.omb.gov>.

National Commission on Terrorist Attacks. (2004). The 9/11 commission report: Final report of the National Commission on Terrorist Attacks upon the United States. New York: W.W. Norton.

Senate Report of the Select Committee on Intelligence. 9 March 2009. 19 March 2009 <http://www.fas.org/irp/congress/2009_rpt/ssci.html>.

Informing Congress of Intelligence Activities

1991 Intelligence Authorization Act (P.L. 102-88).

Bazan, Elizabeth B. and Jennifer K. Elsea, "Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information." Congressional Research Service. 5 January 2006.

"Covert Action: Legislative Background and Possible Policy Questions." Congressional Research Service, 28 January 2008.

Lowenthal, Mark. Intelligence: From Secrets to Policy, 2nd Edition. CQ Press: Washington DC, 2003.

President George W. Bush Radio Address, Dec. 17 2005.

Rindskopf, Elizabeth R. Intelligence Oversight in a Democracy, 11 Hous. J. Int'l L. 30 (1988-1989).

Reid, Edwina Clare. Congressional Intelligence Oversight: Evolution in Progress, 1947 – 2005, Thesis for the Naval Postgraduate School, September 2005.

"Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions." Congressional Research Service, 18 January 2006.

Vandenberg, Lt. Gen. Hoyt. S. "Hearing before the Committee on Expenditures in the Executive Departments, First Session" on H.R. 2319, 27 June 1947.

Covert Action

Bearden, Milt. The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB. New York: Random House, 2003.

"Executive Order: Further Amendments to Executive Order 12333." United States Intelligence Activities. 31 July 2008.

Johnson, Loch K and James Wirtz. Intelligence and National Security. New York: Oxford University Press, 2008.

Kinzer, Stephen. All the Shah's men: an American coup and the roots of Middle East terror. Hoboken, N.J.: John Wiley & Sons, 2008.

Lowenthal, Mark. Intelligence: From Secrets to Policy, 2nd Edition. CQ Press: Washington DC, 2003.

O'Brien, Michael. John F. Kennedy. New York: Macmillan, 2006.

Tenet, George. At the Center of the Storm. New York: Harper Collins, 2007.

Turner, Stansfield. Burn Before Reading: Presidents, CIA Directors, and Secret Intelligence. New York: Hyperion, 2005.

National Intelligence Estimates

"Behind the Iran-Intelligence Reversal," The Wall Street Journal, 8 December 2007.

Bolton, John. "The Flaws in the Iran Report." Washington Post, 6 December 2007.

"Commission to Assess the Ballistic Missile Threat to the United States." 15 July 1998, <http://www.fas.org/irp/threat/missile/rumsfeld/index.html>.

Crail, Peter. "Intel Report Reshapes Iran Sanctions Debate," Arms Control Today, Jan/Feb 2008.

Bruno, Greg. "Backgrounder on National Intelligence Estimates." Council on Foreign Relations. <http://www.cfr.org/publication/7758/national_intelligence_estimates.html#1>.

Department of Defense. "2001 Quadrennial Defense Review." <http://www.defenselink.mil/pubs/pdfs/qdr2001.pdf>.

Director of National Intelligence. "Brief NIC History." 2009. 19 March 2009. <http://www.dni.gov/nic/NIC_history.html#>.

Director of National Intelligence. "Iran: Nuclear Intentions and Capabilities." <http://www.dni.gov/press_releases/20071203_release.pdf>.

Director of National Intelligence. "National Intelligence Estimates and the NIE Process." <http://www.dni.gov/press_releases/20071203_release.pdf>.

Dobbs, Michael. "An Intelligence Turnaround: How Politics Helped Redefine Threat," Washington Post, 14 January 2002.

"Emerging Missile Threats to North America During the Next 15 Years," PS/NIE 95-19, November 1995, < http://www.fas.org/spp/starwars/offdocs/nie9519.htm>.

Hildreth, Steven A. and Amy F. Woolf. National Missile Defense: Issues for Congress. Congressional Research Service, 2 May 2001.

Gates, Robert. "Intelligence Analysis on the Long-Range Missile Threat to the United States," testimony to the Senate Select Committee on Intelligence, 4 December 1996.

Gjelten, Tom. "Iran NIE Reopens Intelligence Debate," NPR. 17 January 2008.

Jervis, Robert. "Reports, Politics, and Intelligence Failures: The Case of Iraq." The Journal of Strategic Studies, vol. 29, no.1 (February 2006).

Jervis, Robert. Perception and Misperception in International Politics. Princeton, NJ: Princeton University Press, 1976.

Kissinger, Henry. "Misreading the Iran Report: Why Spying and Policymaking Don't Mix," Washington Post, 13 December 2007.

Linzer, Dafna. "Iran is Judged 10 years from Nuclear Bomb." Washington Post, 2 August 2005.

Lowenthal, Mark. Intelligence: From Secrets to Policy, 2nd Edition. CQ Press: Washington DC, 2003.

Novak, Robert. "'Arrogant' CIA angers, distresses GOP watchdogs in Congress," Chicago Sun-Times, 24 December 2007.

"Prospects for the Worldwide Development of Ballistic Missile Threats to the Continental United States," NIE 93-17. <http://www.fas.org/irp/threat/nie9317.htm.

Santora, Marc. "Candidates Hold to their Stances on Iran." New York Times, 4 December 2007.

Sanger, David E. and Steven Lee Myers. "Details in Military Notes Led to Shift on Iran, U.S. Says," New York Times, 6 December 2007.

Sanger, David E. and William J. Broad. "Iran is Reported to Test New Centrifuges to Make Atomic Fuel." New York Times, 8 February 2008.

Senate Select Committee on Intelligence, "U.S. Senate Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq." <http://www.globalsecurity.org/intell/library/congress/2004_rpt/iraq-wmd-intell_toc.htm>.

Trachtenberg, David J. "Off the radar." Armed Forces Journal, 2007.

Wright, Robin and Glenn Kessler, "Review of Iran Intelligence to be Sought," Washington Post, 7 December 2007.

Defense Intelligence

The Intelligence Budget Process. United States Intelligence Community. 2009. United States Intelligence Community. 19 March 2009 <http://www.intelligence.gov/2-business_nfip.shtml>.

Lowenthal, Mark. Intelligence: From Secrets to Policy, 2nd Edition. CQ Press: Washington DC, 2003.

"Testimony Before the House Permanent Select Committee on Intelligence." Testimony of William E. Odom. 5 July 2004.

Tyson, Ann Scott. "New Plans Foresee Fighting Terrorism Beyond War Zones." The Washington Post 23 April 2006.

ODNI News Release No. 16-07 "Under Secretary of Defense for Intelligence to be Dual-Hatted as Director of Defense Intelligence." 24 May 2007. Office of the Director of National Intelligence. 19 March 2009 <http://www.dni.gov/press_releases/20070524_release.pdf>.

Richelson, Jeffrey. The U.S. Intelligence Community. 5th Ed. Boulder: Westview Press, 2008.

Tyson, Ann Scott. "New Plans Foresee Fighting Terrorism Beyond War Zones." Washington Post 23 April 2006: A01.

United States Cong. House. Permanent Select Committee on Intelligence. William E. Odom. Testimony. 4 August 2004. 19 March 2009 <http://64.233.169.104/search?q=cache:SFxtmO88yIgJ:www.globalsecurity.org/intell/library/congress/2004_hr/040804-odom.pdf+william+odom+testimony+DIA+intelligence+reform&hl=en&ct=clnk&cd=1&gl=us&client=firefox-a>.

United States Cong. Senate. Select Committee on Intelligence. General Michael V. Hayden, Director, Central Intelligence Agency Statement for the Record. 11 Jan. 2007. 19 March 2009 <https://www.cia.gov/news-information/speeches-testimony/2007/statement_011107.htm>.

Domestic Intelligence

Church Committee Final Report Book III, "The Development of FBI Domestic Intelligence Investigations," 1976.

National Commission on Terrorist Attacks. (2004). The 9/11 commission report: Final report of the National Commission on Terrorist Attacks upon the United States. New York: W.W. Norton.

Treverton, Gregory F. "Balancing Security and Liberty in the War on Terror." Campbell Public Affairs Institute and the Institute for National Security and Counterterrorism, Information Sharing and Homeland Security, Syracuse University: New York, 2004.

Gorman, Siobhan. "Worlds Apart." The National Journal August. 2003 Robert Mueller, speech to the ACLU, June 2003.

Studeman, Michael W. "Strengthening the Shield: U.S. Homeland Security Intelligence." International Journal of Intelligence and Counterintelligence, 20:2.

Kessler, Ronald. "The New Spies." SAIS Review, Winter-Spring 2008.

Intelligence and International Cooperation

Bearden, Milt. The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB. New York: Random House, 2003.

Chertoff, Michael. "Remarks by Homeland Security Secretary Michael Chertoff To The Heyman Fellows At Yale University On "Confronting The Threats To Our Homeland." 7 April 2008.

Lowenthal, Mark. Intelligence: From Secrets to Policy, 2nd Edition. CQ Press: Washington DC, 2003.

Richelson, Jeffrey. The U.S. Intelligence Community. 5th Ed. Boulder: Westview Press, 2008.

Tenet, George. At the Center of the Storm. New York: Harper Collins, 2007.

Intelligence Reform

Cumming, Alfred, FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress, CRS Report 4

August 2004. Accessed at www.fas.org/irp/crs/RL32336.pdf.

Fingar, Thomas, "Intelligence Reform," Council on Foreign Relations, 18 March 2008. Accessed at <http://www.cfr.org/publication/15754/intelligence_reform_rush_transcript_federal_news_service.html>.

Graham, Bob, et al "World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism," Vintage Books: New York.

Intelligence Reform and Terrorism Prevention Act of 2004 (H.Rpt. 108-796 -) <http://www.gpoaccess.gov/serialset/creports/intel_reform.html>.

National Intelligence Strategy for the United States of America, October 2005. <http://www.dni.gov/publications/NISOctober2005.pdf>.

"Mapping the Global Future: Report of the National Intelligence Council's 2020 Project Based on Consultations With Nongovernment Experts Around the World." National Intelligence Council. December 2004. <http://www.cia.gov/nic/NIC_globaltrend2020.html#contents>.

Progress of the DNI in Implementing the IRTPA May 2006. Accessed at <http://74.125.47.132/search?q=cache:w431Mufc-eIJ:www.fas.org/irp/dni/implement.html+what+the+IRTPA+changed&hl=en&ct=clnk&cd=15&gl=us&client=firefox-a>.

Report to the President of the United States, The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. 31 March 2005 <http://www.wmd.gov/report/>.

Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq. 19 March 2009. <http://www.gpoaccess.gov/serialset/creports/iraq.html>.

Walker, David M., Comptroller General of the United States United States Government Accountability Office GAO Testimony.

"GAO Can Assist the Congress and the Intelligence Community on Management Reform Initiatives." 29 February 2008. 19 March 2009 <http://74.125.95.132/search?q=cache:HJ3-8l0V81cJ:www.gao.gov/cgi-bin/getrpt%3FGAO-08-413T+intelligence+reform&hl=en&ct=clnk&cd=34&gl=us&client=firefox-a>.

White House Fact Sheet: Reforming and Strengthening Intelligence Services, 8 September 2004. Accessed at <http://74.125.47.132/search?q=cache:OpKFjXtBcvMJ:merln.ndu.edu/archivepdf/nss/WH/20040908-5.pdf+Reforming+and+Strengthening+Intelligence+Services&hl=en&ct=clnk&cd=1&gl=us&client=firefox-a>.

Interrogations and Intelligence

Ayres, Thomas. ""Six Floors" of Detainee Operations in the Post-9/11 World." Parameters, Autumn 2005.

The Charlie Rose Show. "Interview with Michael Hayden." 23 October 2007.

DeYoung, Karen. "Bush Approves New CIA Methods." Washington Post, 21 July 2007.

Eggen, Dan and Walter Pincus. "FBI, CIA Debate Significance of Terror Suspect." Washington Post. 18 December 2007.

FM 2-22.3 Human Intelligence Collector Operations. U.S. Army. September 2006.

FM 34-52 Intelligence Interrogation. Department of the Army. May 1987.

Goldsmith, Jack. The Terror Presidency. New York: W.W. Norton, 2007.

Jehl, Douglas. "Iraq War Intelligence Linked to Coercion" International Herald-Tribune. 9 December 2005.

Myers, Steven. "Veto of Bill on C.I.A. Tactics Affirms Bush's Legacy." New York Times, 9 March 2008.

"President Discusses Creation of Military Commissions to Try Suspected Terrorists" The White House. 6 September 2006.

Ross, Brian and Richard Esposito. "CIA's Harsh Interrogation Techniques Described" ABC News, 18 November 2005.

Shane, Scott, David Johnston and James Risen "Secret U.S. Endorsement of Severe Interrogations." New York Times, 4 October 2007.

Suleman, Arsalan M. "Detainee Treatment Act of 2005." Harvard Human Rights Journal. Issue 19, Spring 2006.

"U.S. Army/Marine Corps Counterinsurgency Field Manual." University of Chicago Press, 2007.

Warrick, Joby. "CIA Tactics Endorsed in Secret Memos." Washington Post, 15 October 2008.

Electronic Surveillance and FISA

Bazan, Elizabeth B. The Foreign Intelligence Surveillance Act: Comparison of the Senate Amendment to H.R. 3773 and the House Amendment to the Senate Amendment to H.R. 3773, 12 June 2008. Accessed 19 March 2009 <http://www.fas.org/sgp/crs/intel/RL34533.pdf>.

Congressional Record (House) 20 June 2008. 19 March 2009. <http://www.fas.org/irp/congress/2008_cr/house-fisa.html>.

Congressional Record (Senate) 9 July 2008. FISA Amendments Act of 2008, 19 March 2009 <http://www.fas.org/irp/congress/2008_cr/fisa070908.html>.

Hess, Pamela (2008-06-20). "House immunizes telecoms from lawsuits". Washington Times 20 June 2008. Accessed 19 March 2009 <http://www.washingtontimes.com/news/2008/jun/20/house-immunizes-telecoms-from-lawsuits>.

Liptak, Adam. "U.S. Defends Surveillance to 3 Skeptical Judges." New York Times. 16 August 2007.

Lowenthal, Mark. Intelligence: From Secrets to Policy. 4th ed. Washington, D.C.: CQ Press, 2009.

Risen, James and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." New York Times. 16 December 2005.

"H.R.3162: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled as Agreed to or Passed by Both House and Senate)" Library of Congress. <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:>.

Cyber Security and the Intelligence Community

"Annual Report to Congress: Military Power of the People's Republic of China 2008." Department of Defense. <http://www.defenselink.mil/pubs/pdfs/China_Military_Report_08.pdf>.

Bain, Ben. "Number of Reported Cyber Incidents Jumps." Federal Computer Week. 17 Feb 2009.

"China Denies Hacking U.S. Computers." AP, 12 June 2008.

Department of Homeland Security. "National Strategy to Secure Cyberspace." <http://www.dhs.gov/xprevprot/programs/editorial_0329.shtm>.

Department of Homeland Security. "US-CERT." <http://www.us-cert.gov>.

Director of National Intelligence. "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee." 27 February 2008.

"Estonia's Web Sites Crippled by Russian Hackers." FOX News. 18 May 2007.

Harris, Shane. "Chinese hackers pose serious danger to U.S. computer networks." National Journal. 29 May 2008.

Morozov, Evgeny. "The Kremlin's Virtual Army." Foreign Policy. August 2008.

Shachtman, Noah. "Russian Coder: I Hacked Georgia's Sites in Cyberwar." Wired. 23 October 2008.

Shalal-Esa, Andrea. "U.S. working to respond to growing cyber attacks." Reuters, 27 November 2007.

Somashekhar, Sandhya. "Wolf Warns of Foreign Attacks on Computers." Washington Post, 12 June 2008.

Overhead Surveillance

Beizer, Doug. "BAE to Develop Surveillance System." Washington Post. 12 November 2007.

Brook, Tom Vanden. "Spy Technology Caught in Military Turf Battle." USA Today. 17 October 2007.

Butler, Amy. "Panel Wants Massive Milspace Reshuffling." Aviation Week. 14 August 2008.

Doty, John. "NGA Meets Diverse Demands with Commercial Imagery." Earth Imaging Journal. 19 March 2009 <http://www.eijournal.com/NGA.asp>.

Flaherty, Anne and Pamela Hess. "U.S. Plans New Spy Satellite Program." Associated Press. 1 Dec 2007.

Krauss, Leah. "Analysis: UAV Sales Help IAI Bottom Line." UPI Security and Terrorism. 29 November 2007.

Lowenthal, Mark. Intelligence: From Secrets to Policy, 2nd Edition. CQ Press: Washington DC, 2003.

Matthews,William. "China Sat Test Spurs U.S. To Boost Space Spending." Defense News. 11 June 2007.

Pincus, Walter. "Gadgets That Collect Information Are Also Gathering Success." Washington Post. 15 September 2008.

Richelson, Jeffrey. The U.S. Intelligence Community. 5th Ed. Boulder: Westview Press, 2008.

Senate Committee on Armed Services. Intelligence Authorization Act For Fiscal Year 2008. June 2007.

Shalal-Esa, Andrea. "Pentagon sees expanding use of satellite imagery" Reuters, 1 October 2008.

Taubman, Philip. "In Death of Spy Satellite Program, Lofty Plans and Unrealistic Bids." New York Times. 11 November 2007.

"Teal Group Predicts Worldwide UAV Market Will Reach Nearly $55 Billion in Its 2008 UAV Market Profile and Forecast." PRNewswire. 29 November 2007.

The National Interest, Energy Security and the Intelligence Community

Butts, Kent Hughes and Arthur L. Bradshaw Jr. "Military Education Workshop Addresses Threats to Stability and Security." Issue Paper, Center for Strategic Leadership, U.S. Army War College, Aug 2007, Vol. 8-07.

"NIC Chairman: Intelligence Challenges Through 2015." Remarks by John C. Gannon, Chairman, National Intelligence Council to the Columbus Council on World Affairs, 27 April 2000.

Central Intelligence Agency Support to National Policy. 2009. Central Intelligence Agency. Accessed 19 March 2009 <https://www.cia.gov/library/reports/archived-reports-1/Ann_Rpt_2003/snp.html>.

CFR, National Security Consequences of U.S. Oil Dependency, Independent Task force report No. 58, 2006.

Climate Change NIE study commissioned by NIC done through the Columbia University Center for International Earth Science Information Network (CIESIN) 19 March 2009 <http://www.ciesin.columbia.edu>.

Congressional Record: Senate Statements on Introduced Bills and Joint Resolutions. 13 June 2007. 19 March 2009 <http://www.fas.org/irp/congress/2007_cr/s1613.html>.

Dreyfuss, Robert. "Company Spies." Mother Jones, May/June 1994. 19 March 2009. <http://www.motherjones.com/politics/1994/05/company-spies>.

Kalicki, Jan H. and David L. Goldwyn (eds.) Energy & Security: Toward a New Foreign Policy Strategy. Johns Hopkins University Press, 2005.

Mapping the Global Future: Report of the National Intelligence Council's 2020 Project. 19 March 2009. <http://www.dni.gov/nic/NIC_2020_project.html>.

National Intelligence Council. 2009. National Intelligence Council. 19 March 2009. <http://www.dni.gov/nic/NIC_home.html>.

Office of the Director of National Intelligence. 2009. Office of the Director of National Intelligence. 19 March 2009. <http://www.dni.gov>.

Riley, Sheila. "Cyber rules guard grid." Electronic Engineering Times 4 February 2008.

Weighing Intelligence for Smarter Energy Act (WISE Act) S.1613, 2007.

Terrorist Safehavens and the Intelligence Community

Coates, Sam and Jeremy Page. "Pakistan 'linked to 75% of all UK Terror Plots', warns Gordon Brown." Times of London, 15 December 2008.

Defense Intelligence Agency. "Current and Projected National Security Threats to the United States." Testimony by Vice Admiral Lowell E. Jacoby, 24 February 2004.

DeYoung, Karen. "World Bank Lists Failing Nations That Can Breed Global Terrorism." The Washington Post, 15 September 2006.

"Exclusive: CIA Aircraft Kills Terrorist" ABC News. 13 May 2005.

"FATA Morgana," The Economist 18 September 2008.

Filkins, Dexter. "Right at the Edge," The New York Times Magazine. 5 September 2008.

Forero, Juan. "In Columbia Jungle Ruse, U.S. Played A Quiet Role." Washington Post. 9 July 2008.

"Fragile and Conflict-Affected Countries." The World Bank. 24 September 2008. <http://web.worldbank.org/WBSITE/EXTERNAL/PROJECTS/STRATEGIES/EXTLICUS/0,,menuPK:511784~pagePK:64171540~piPK:64171528~theSitePK:511778,00.html>.

Jones, Owen Bennett. Pakistan: Eye of the Storm. New Haven: Yale University Press, 2002.

"How to Beat the Terrorists," The Economist. 23 September 2008.

Martin, David. "Europe Terror Plots Trace Back to Pakistan." CBS News. 25 January 2008.

Menkhaus, Ken. "Terrorist Activities in Ungoverned Spaces: Evidence and Observations from the Horn of Africa." paper prepared for the Southern Africa and International Terrorism conference, January 2007.

"Pakistan Recovers 'U.S. Spy Drone,'" BBC News, 24 September 2008.

Weber, Max. "Politics as a Vocation." Vocation Lectures. University of Munich. 1918.

"The U.S. Air Force Remotely Piloted Aircraft and Unmanned Aerial Vehicle Strategic Vision" U.S. Air Force. 2005. <http://www.af.mil/shared/media/document/AFD-060322-009.pdf>.

"A Wild Frontier," The Economist. 18 September 2008.

The Role of Private Corporations in the Intelligence Community

"CIA, NRO, and Air Force Celebrate the U-2: A Revolution in Intelligence." Central Intelligence Agency, 28 September 1998. <https://www.cia.gov/news-information/press-releases-statements/press-release-archive-1998/pr092898.html>.

Clarke, Richard. Your Government Failed You. New York: Harper Collins, 2008.

Fainaru, Steve. "Where Military Rules Don't Apply." Washington Post, 20 September 2007. A01.

Hillhouse R.J. "Outsourcing Intelligence." The Nation. 24 July 2007.

Holmes, Erik. "Bringing UAVs to Life." Air Force Times. 7 November 2008.

Pincus, Walter. "Defense Agency Proposes Outsourcing More Spying." Washington Post, 19 August 2007. A03.

Scahill, Jeremy. Blackwater: the Rise of the World's Most Powerful Mercenary Army." New York: Nation Books, 2007.

Shorrock, Tim. "Former High-ranking Bush Officials Enjoy War Profits." Salon Magazine. 29 May 2008.

Statement by Ellen Cioccio, Acting Director of Public Affairs, ODNI 19 June 2007. <http://www.dni.gov/announcements/20070619_announcement.pdf>.

Senate Select Committee on Intelligence Report 110-75, May 31, 2007.

U.S. Army Report, "The Investigation of Intelligence Activities at Abu Ghraib," p. 18. <http://www4.army.mil/ocpa/reports/ar15-6/index.html>.

The USA-PATRIOT Act

Abramson, Larry and Maria Godoy. "The Patriot Act: Key Controversies." NPR. 14 February 2006.

"Bush Officials Urge Congress to Boost Patriot Act Powers." Washington Times. 6 April 2005.

"H.R.3162: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled as Agreed to or Passed by Both House and Senate)" Library of Congress. <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:>.

Lichtblau, Eric. "A Nation At War: Liberty And Security; Republicans Want Terrorism Law Made Permanent." New York Times. 9 April 2003.

Schmitt, Richard. "Patriot Act is called vital." Los Angeles Times. 6 April 2005.

"USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (S. 2271)" Congressional Research Service, 21 February 2006.

State and Local Fusion Centers

9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition: U.S. Government Printing Office Washington D.C., 22 July 2004. 19 March 2009 <http://www.9-11commission.gov/report/911Report.pdf>.

"Fusion Centers: Giving Cops Too Much Information?" Time. 9 March 2009.

Fusion Center Guidelines: Developing and Sharing Information in a New Era. 2005. 19 March 2009 <http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf>.

Kaplan, Eben, "Fusion Centers" Council on Foreign Relations. 22 February 2007. 19 March 2009 <http://www.cfr.org/publication/12689>.

The Privacy Act of 1974 5 U.S.C. § 552a. 19 March 2009. <http://www.usdoj.gov/04foia/privstat.htm>.

U.S. Department of Homeland Security State and Local Fusion Centers. 2009. U.S. Department of Homeland Security. 19 March 2009 <http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm>.

U.S. Department of Justice, Office of Justice Programs. 2009. U.S. Department of Justice. 19 March 2009 <http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181>.

Acknowledgments

This book is the product of numerous individuals researching the murky and often complex interactions between Congress and the Intelligence Community. We would first like to thank **Graham Allison** and **Senator Bob Graham**, whose thoughtful insight played a critical role in shaping this publication. The Belfer Center's Intelligence and Policy Project Fellow **Hope LeBeau** ably managed the Project and oversaw the book's overall production, while **Susan Sypko** and **Ya'ara Barnoon** provided outstanding research in its early stages.

We are extremely grateful to our colleagues who provided insight, counsel, research and recommendations, including: **CDR Todd C. Huntley**, **Tamara Klajn**, **Sarah Miller**, **Siobhan O'Neil**, **Edward Price**, **Jessica Reitz**, **JP Schnapper-Casteras**, **David Sklar** & **Alex Spisak**. We would like to give special thanks to our Kennedy School colleagues **Cynthia Lobosky**, **Arnold Bogis** and **Joe Costa** who provided endless edits, as well as our graphic designer **Timothy Duffy**.

We would finally like to thank the many current and former U.S. government officials who generously gave their time and thoughts to help us better understand these significant national security issues. Many of these experts prefer to remain anonymous, but they have our appreciation.

This briefing book would not have been possible without the sponsorship of the Office of the Director of National Intelligence. In the interest of full disclosure, this publication was submitted for pre-publication reviews to the Central Intelligence Agency to ensure that no classified information was accidentally disclosed. However, CIA's review did not shape the book's scope, tone, or subject material; rather, the authors remain solely responsible for this publication's content.

The views expressed are those of the authors and do not represent the views of the U.S. Government.

About the Authors

Eric Rosenbach

Eric Rosenbach is the Executive Director of the Belfer Center for Science and International Affairs at the Harvard Kennedy School.

Prior to his work at the Belfer Center, Rosenbach was a professional staff member on the Senate Select Committee on Intelligence and served as the national security advisor for U.S. Senator Chuck Hagel.

On the Intelligence Committee, Rosenbach provided oversight of the intelligence community's counterterrorism efforts. Rosenbach led and authored two formal Senate Intelligence Committee investigations of prewar intelligence on Iraq, entitled Postwar Findings about Iraq's Links to Terrorism and Prewar Intelligence about Postwar Iraq.

Rosenbach served as an active-duty military intelligence officer supporting post-conflict operations in the Balkans. As a commander, he was awarded the Meritorious Service Medal. The Director of Central Intelligence named his unit as the top intelligence organization in the U.S. military for two consecutive years.

Rosenbach co-authored a book on counter-terrorism policy with Richard A. Clarke and other experts in 2004. He recently co-edited a book on military leadership entitled *In Pursuit of Excellence*.

He completed a juris doctor in national security law at Georgetown, masters in public policy at the Harvard Kennedy School and bachelor of arts at Davidson College. As a Fulbright Scholar in Eastern Europe, Rosenbach conducted post-graduate research on privatization programs.

Aki J. Peritz

Aki J. Peritz is an Associate at the Belfer Center for Science and International Affairs at the Harvard Kennedy School of Government. He holds a Master of Arts from the University of Washington and a Bachelor of Arts from the University of Pennsylvania. He currently lives with his wife, Dana, in Cambridge, MA.