Intelligence Secrecy and Transparency: Finding the Proper Balance from the War of Independence to the War on Terror

Strategic Insights, Volume VI, Issue 3 (May 2007)

by CAPT Timothy J. Doorey, USN

Strategic Insights is a bi-monthly electronic journal produced by the Center for Contemporary Conflict at the Naval Postgraduate School in Monterey, California. The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.

The necessity of procuring good intelligence is apparent & need not be further urged – All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, success depends in Most Enterprizes of the kind, & for want of it, they are generally defeated, however well planned…."

— General George Washington to Col. Elias Dayton, July 26: 1777.[1]

Introduction

It is comforting to know that the tension between America's desire for transparency in its government's activities and the secrecy required for effective intelligence operations predates the Republic. For much of its history, America ingeniously dealt with the transparency vice secrecy dilemma by either disbanding or shrinking its small intelligence services after every military conflict. As Mark Lowenthal points out, the United States did not have a national intelligence organization for 170 years of its existence.[2] Indeed, it was not until the 1880s that the U.S. Navy and Army, alarmed by the rapid technological advances of their European counterparts, established small and permanent intelligence organizations with dedicated budgets and personnel. Since these military intelligence organizations were focused primarily on foreign military capabilities, and operated for the most part overseas, they received little media or congressional attention.

The modern U.S. Intelligence Community (IC) can trace its history back to 1940; and, especially with the passing of the National Security Act of 1947.[3] In the wake of the successful Japanese surprise attack on Pearl Harbor, and the emerging Soviet conventional and eventual nuclear threat in the post-World War II era, successive presidents built and maintained robust intelligence capabilities, which today consist of seventeen agencies, with approximately 100,000 employees and budgets well over $44 billion a year.[4]

For clarity, this article assumes that by intelligence secrecy, one means that, with few exceptions, the executive branch and its subordinate intelligence agencies decide who will be given access to sensitive intelligence on sources and methods, and at times, covert operations. Conversely, the demand for greater transparency and oversight of U.S. intelligence activities would come from an American public suspicious of such concentration of power within the executive branch. Intelligence transparency therefore means a greater oversight role for the American public's

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intelligence Secrecy and Transparency: Finding the Proper Balance from the War of Independence to the War on Terror	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Contemporary Conflict,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**13**	

representatives in the legislative and judicial branches of government, as well as the media, to ensure the U.S. IC is carrying out its mission effectively and efficiently, legally, and in a manner consistent with the values, rights and privacy of its citizens. The U.S. Government's challenge is therefore to find the proper balance, under our Constitution, between intelligence secrecy, accountability and transparency.

Despite America's long history of checks and balances among its executive, legislative and judicial branches of government, the concept of separation of powers as it pertains to intelligence activities is a relatively new phenomenon. The historical record of the executive branch complying with legislative and judicial oversight of intelligence activities dates back only to the mid-1970s. Since then, the process has been uneven at best. While General George Washington worked closely with the pre-Constitutional Congress during the Revolutionary War (both maintained complementary intelligence organizations), after that period, the executive branch for the most part kept Congress out of intelligence affairs until the mid-1970s.[5] Over the decades, Congress occasionally made feeble attempts at oversight, specifically to see how the money it had appropriated for secret, intelligence-related activities was being spent, only to be rebuffed by the President. For example, in 1846, the House of Representatives issued a resolution for President James K. Polk to produce records of the Secret Service Fund expenditures during the previous administration. Polk refused on the grounds of national security, and Congress did not pursue the issue.[6]

The Need for Secrecy

George Washington's wartime plea aside, Americans have always been wary of professional intelligence services insisting that their activities remain secret, even from other branches of the U.S. Government. Such secrecy seems at odds with the America's democratic principles, specifically the need for openness and transparency in government affairs. This skepticism proved justified when in the 1970s and 80s, the press and Congress uncovered numerous examples of the U.S. IC engaging in illegal and ethically-suspect activities.[7]

Many citizens today are again questioning the IC's activities, including its competence and professionalism after learning about serious intelligence failures leading up to the 9/11 attacks in September 2001, and prior to the Iraq war in March 2003. These very public failures, combined with controversial practices such as renditions and detentions of terrorism suspects, warrant-less searches and widespread eavesdropping against U.S. citizens, have sparked greater demand for transparency in intelligence-related activities.[8]

However, secrecy remains a key component of the United States' IC's effectiveness. Compromised sensitive technical and human intelligence "sources and methods" will often lead to either the loss of that specific source of intelligence, or worse, the opportunity for our targeted adversary to pass phony or misleading information through the compromised sources as part of an elaborate deception operation. Two experts on intelligence, Abram N. Shulsky and Gary J. Schmitt, point out that secrecy is essential in all aspects of intelligence since the target is a human adversary who is fighting back. They point out that, "One side's intelligence failure is likely to be another side's counterintelligence success."[9]

A cursory review of intelligence activities during World War II clearly shows the critical importance of secrecy during wartime. Key technical intelligence collection capabilities, such as the massive British communication intelligence (COMINT) collection and decryption effort against Hitler's war machine, codenamed ULTRA, or America's counterpart effort to collect and break Imperial Japan's PURPLE code, codenamed MAGIC, were instrumental in assisting the United States and its allies prevail in World War II. Allied successes at D-Day, the Battle of Midway and countless other battles in both the European and Pacific theaters can be traced backed to the intelligence

advantages afforded the allies, and were only possible because the ULTRA and MAGIC COMINT programs remained secret throughout the war.[10]

During the Cold War, secret technical intelligence capabilities allowed us to penetrate the closed Soviet bloc. The brilliant aircraft designer, Clarence “Kelly” Johnson, and his team at Lockheed Martin’s famous “skunk works,” working with the CIA and the Pentagon, developed both the U-2 and SR-71 Blackbird state-of-the-art imagery intelligence (IMINT) reconnaissance aircraft in secret in the 1950s. After testing, the U-2 began secret reconnaissance flights over the Soviet Union until an aircraft, piloted by Gary Frances Powers, was shot down on one such mission in 1960. Despite that setback, in October 1962, U.S. Air Force U-2 reconnaissance aircraft played a pivotal role in uncovering the secret deployment of Soviet Intermediate Range Ballistic Missiles (IRBMs) to Cuba capable of delivering nuclear warheads against major cites on the U.S. eastern seaboard. That secretly-collected intelligence allowed the Kennedy administration to conduct timely diplomatic intervention which supported a peaceful resolution of the Cuban Missile Crisis with the Soviet Union. Despite its advanced age, updated U-2 aircraft remain operational today, although with significantly upgraded sensor capabilities that remain secret.[11]

In the late 1950s, the Eisenhower administration first authorized the CIA and USAF to begin building reconnaissance satellites with secret collection capabilities. Over the past five decades, these satellites have assisted U.S. intelligence collection efforts around the world, especially in denied areas where other forms of collection were impractical. As was true in World War II, secrecy about the capabilities of these high-tech collection platforms, and the targets they are tasked to collect against, is essential to prevent the targeted adversaries from implementing countermeasures such as camouflage and other forms of deception.

An example of the high cost associated with the compromise of a sophisticated technical intelligence collection effort is Project Jennifer, also known as the Hughes Glomar Explorer. This specially-designed marine salvage ship was built in 1973 by Sun Shipbuilding and Drydock Company to retrieve a sunken Soviet Golf-II Class ballistic missile submarine lost on April 11, 1968, 750 miles northwest of Hawaii at an approximate depth of 17,000 feet. According to an account by the Federation of American Scientists, the Glomar Explorer cost in excess of $200 million to build (a contemporaneous *Time Magazine* article placed the cost of the entire operation at $350 million). The Glomar Explorer made only one voyage to collect the submarine in June 1974. According the press, the mission was only partially successful before the Los Angeles Times broke the story in February 1975. With its cover blown, the Glomar Explorer’s brief career as an expensive covert intelligence collection platform was over.[12]

The compromise of costly technical collection sources and methods is usually measured in dollars and lost intelligence collection opportunities; whereas the compromise of human intelligence (HUMINT) agents working for the U.S. IC, or our allies, is often measured in lost lives, and the unwillingness of other potential agents around the world to work with U.S. intelligence. Former CIA spy Aldrich Ames identified 25 CIA “human assets” to the Soviet KGB in the mid-1980s in return for $ 2.7 million; most of those agents Ames betrayed—who were unable to escape to the West—were tried and executed.”[13] In addition to Aldrich Ames, there have been a number of high-profile cases of treason involving individuals working for the U.S. IC. On May 14, 2002, career FBI agent and counter-intelligence expert, Robert Hansen, pleaded guilty to fifteen counts of espionage and conspiracy. The previous year, one of the two charges formally laid out against him in an Alexandria, Virginia courtroom was that he revealed the identities of three KGB men in October 1989 who worked as double agents for the United States. The CIA believes that the three were subsequently executed.[14] Such widely publicized examples of U.S. intelligence unable to protect the identities of their human sources can have had a chilling effect on the willingness of others to cooperate with U.S. intelligence. The risk of compromise is just too great.

While secrecy is a key ingredient in intelligence collection, its role in analysis is more complex, and at times, counterproductive. Like other living systems, nations and non-state actors are

complex entities. Understanding how they work, think, communicate, make decisions and interact with those around them usually takes a collective effort, pulling together the knowledge of many experts with various backgrounds. Many such experts may not have security clearances, and may not be able to obtain them due to many circumstances. Excessive secrecy will, by definition, limit the number and type of experts who can participate in the all-source analysis, which can undermine the quality of the final intelligence product. Excessive secrecy will limit the information one can apply to a specific problem thus forcing less-knowledgeable analysts to wittingly or unwittingly fill in the blanks with their biases and, at times, secret information of questionable reliability. The question remains, how much should the IC limit participation in its analytical efforts in order to maintain secrecy? At what point does the quest for secrecy become self-defeating?

Open Source Intelligence (OSINT) has always contributed to all-source analysis, yet the information revolution has added a major new dimension to the battle between transparency and secrecy. Like Sam Colt's six-shooter of the Old West, the Internet and powerful, publicly-available search engines are the new "great equalizers" of the 21st Century information wars. These widely available information technologies have eroded much of the information advantage once enjoyed by only a small number of wealthy countries with large intelligence bureaucracies capable of sifting though tons of printed material or terabytes of information on massive databases.

For example, Google Earth, which was unveiled in June 2005, has satellite imagery, mapping overlays, GPS features, and various other toolkits U.S. intelligence analysts would have drooled over in the 1990s. According to Google's John Hanke, "ten years ago, this technology was the exclusive province of the U.S. IC. Five years ago, it cost $14,000 for a single satellite image. Now there's free, global high-resolution imagery."[15] Heady stuff indeed, but what it also means is that any al-Qaida terrorist with a hotmail account, from any Internet café around the world, can now access information that previously was the purview of only a handful of large state actors. Earlier this year, British forces in Basra, Iraq claimed they found sets of photographs of Google Earth mapping tool during raids of suspected insurgents' homes. The annotated photographs were of the palace complex in Basra where over 1,000 British soldiers are stationed.[16]

Even the U.S. IC is struggling to better leverage this tsunami of open source information, while at the same time maintaining the secrecy of its remaining technical and human sources and methods. It is becoming increasingly clear that those precious few secret technical and human sources and methods are the only remaining intelligence advantages that the United States and its allies have over a wide range of actual and potential state and non-state adversaries.

The Case for Transparency

All major democratic government activities require oversight and accountability, both internal and external, to ensure they are performing their mission competently, operating within the law, and using the taxpayers' resources in an efficient and effective manner. This oversight requirement is essential for the intelligence community since most of its activities are conducted under the cloak of secrecy; not subject to many of the traditional safeguards common in other governmental agencies. For much of the U.S. IC's history, Congress, the media and the American publics' attitude towards intelligence varied from trust, disinterest to occasional outrage when scandals were revealed. As the late LTG Vernon Walters, USA (ret.), former U.S. Ambassador to the United Nations and Deputy Director of Central Intelligence, once said, "Americans have always had an ambivalent attitude toward intelligence. When they feel threatened, they want a lot of it, and when they don't, they regard the whole thing as somewhat immoral."[17]

Following September 11th, the American public and their elected officials definitely wanted a lot of it, and they were more than willing to suspend traditional safeguards to civil liberties to make sure they got it. Congress passed, with virtually no debate, the USA PATRIOT ACT just 45 days after September 11th attacks. Few, at the time, questioned the Intelligence Community's need for

expanded powers or complete secrecy to aggressively pursue the al-Qaeda terrorists responsible for the 9/11 attacks. Many in Congress willingly ceded their traditional oversight responsibilities to the executive branch in an effort to enhance the effectiveness and efficiency of the interagency intelligence fight against a pernicious enemy they did not understand. However, following the revelations in the *Final Report of the National Commission on Terrorist Attacks Upon the United States*, better known as 9/11 Commission, as well as the U.S. failure to find Weapons of Mass Destruction (WMD) in Iraq in 2003, and numerous media reports of warrant-less wiretaps and other forms of "data-mining" against U.S. citizens, the American public and Congress are once again demanding more congressional oversight of the U.S. IC.

A *Washington Post-ABC News Poll* conducted in December 2006, showed 66 percent of the 1,005-person random sample questioned believe that the FBI and other agencies were "intruding on some Americans' privacy rights" in terrorism investigations, up from 58 percent in September 2003.[18] A subset of those polled showed 52 percent wanted congressional hearings on how the Bush Administration handles surveillance, detainees and other terrorism-related issues.[19]

As for the IC's effectiveness, many citizens and their elected officials were justifiably outraged by many of the 9/11 Commission findings. The bipartisan Commission, mandated by Congress, issued a report that served as an exposé of the IC's handling of the intelligence leading up to the attacks on September 11th.[20] The Commission's findings provided the impetus for executive and legislative intelligence reform efforts, specifically the creation of the Office of the Director of National Intelligence (ODNI) in December 2004.

On the heels of 9/11, another serious "intelligence failure" was the IC's pre-war assessment of Saddam Hussein's chemical, biological and nuclear "weapons of mass destruction" (WMD) programs. The IC's findings were formally presented in an October 2002 National Intelligence Estimate (NIE), requested by Congress, prior to the House and Senate vote to authorize the President to use force against Iraq. Secretary of State Colin Powell's February 5, 2003 address to the United Nations contained many of the same intelligence sources used in the NIE to make the case for war to the world. It was only after the invasion that the public learned that many of the sources used in the NIE and then Secretary of State's U.N. speech were known fabricators, and that the all-source analysis was sloppy at best.[21]

Several congressional commissions were established to investigate what went wrong. On February 6, 2004, Executive Order 13328 established the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, commonly referred to as the WMD Commission. At the time the WMD Commission was reviewing the IC failings until it issued its final report on March 31, 2005, the IC's Iraq Survey Group (ISG) was also conducting a thorough search for WMD in Iraq. According to a May 30, 2003 briefing by Dr. Stephen A. Cambone, the Pentagon's Undersecretary of Defense for Intelligence (USDI), and Major General Keith Dayton, U.S. Army, commander of the ISG, the ISG was manned by approximately 1,300 and 1,400 people. This massive effort was conducted following the 75th Exploitation Task Force's effort which had already searched 300 sensitive sites. The ISG issued its final report on September 30th, 2004.[22] The massive ISG effort to find WMD in Iraq coincided with the growth and lethality of the insurgency, begging the question: what were the opportunity costs of having so many intelligence personal diverted to the WMD search in Iraq for so long?

Nor has the controversy over Iraq-related intelligence been limited to the WMD issue. On March 15, 2006, Congress established an independent and bipartisan Iraq Study Group co-chaired by former Secretary of State James Baker, a Republican, and former Democratic congressman, Lee Hamilton, to independently assess the war in Iraq and to offer policy recommendations. The Iraq Study Group issued its final report on December 6, 2006. Buried deep within their final report were troubling findings about the quality of the U.S. intelligence effort in Iraq. While the report stated that tactical intelligence was good and at times superb, "our government still does not understand very well either the insurgency in Iraq or the militias."[23] The Study Group found a

number of human intelligence and analytical shortfalls, and three of the seventy-nine total recommendations it offered specifically dealt with ways the IC could enhance its intelligence effort in Iraq.[24]

Clearly secrecy alone did not aid the intelligence efforts mentioned above, and may have delayed the proper diagnosis of problems and remedial initiatives. If the Iraq Study Group was still finding problems as late as December 2006 that internal IC oversight was failing to uncover much less correct, secrecy may have unnecessarily prolonged serious deficiencies in personnel management and resource allocation, collection, and analysis.

In addition to privacy and performance issues, the IC's secret budgets, involving tens of billions of dollars, require vigilant internal and external oversight to prevent incompetent or corrupt officials from misappropriating funds. While the overall IC budget remains classified, it is likely greater than the last time it was made public in 1997. At the time, George Tenet, then the Director of Central Intelligence, in a response to a Freedom of Information Act suit, revealed that overall intelligence spending for fiscal 1998 was $26.6 billion.[25] By comparison, NASA's proposed budget for FY 2008 was $18.9 billion.[26]

There is mounting evidence that a few senior officials misused secrecy to hide fraud and corruption during the rapid post-9/11 expansion of intelligence activities. On February 13, 2007, a federal grand jury in San Diego indicted Brent R. Wilkes, a Californian businessman, and Kyle "Dusty" Foggo, the former third-ranking official at the CIA, on fraud, conspiracy and money laundering charges involving former Representative Randy "Duke" Cunningham.[27] In November 2005, Cunningham was forced to resign from the House after pleading guilty to taking bribes and is now serving up to an eight-year prison term. Walter Pincus of the *Washington Post* notes that congressional investigators found that Cunningham "channeled more than $70 million in Pentagon and intelligence agency contracts to two companies which paid him bribes."[28] According to the executive summary of the investigation by the House Permanent Select Committee on Intelligence (HPSCI), Cunningham's illegal activities required the "cooperation or at least the non-interference of many people"[29] Pincus claims several of the questionable contracts involved the Pentagon's newest and fastest-growing intelligence agency, the Counterintelligence Field Activity (CIFA), which was established in 2002 to coordinate the protection of defense facilities and personnel at home and abroad from terrorist attacks. CIFA's budget is secret.[30] Of note, according to Pincus, this same organization was at the center of a storm in November 2005, when it was learned "The Pentagon pushed legislation on Capitol Hill that would create an intelligence exception to the Privacy Act, allowing the FBI and others to share information gathered about U.S. citizens with the Pentagon, CIA and other intelligence agencies, as long as the data is deemed to be related to foreign intelligence."[31] At the time, one member of the Senate Select Committee on Intelligence (SSCI), Senator Ron Widen (D-OR) claimed, "We are deputizing the military to spy on law-abiding Americans in America. This is a huge leap without even a [congressional] hearing."[32]

Thus, this new intelligence agency, CIFA, created only in 2002, has already found itself embroiled in two of the three main reasons for greater transparency and intelligence oversight: ensuring the privacy of law-abiding citizens and fiscal accountability.

Perhaps the most compelling reason for greater transparency in the intelligence process is to enhance the credibility of its final product. If intelligence is to be used to drive policy decisions, it must be credible for policymakers, legislators and citizens to sacrifice their blood and treasure to implement intelligence-driven strategies.

Whence the Threat to Intelligence Secrecy?

All intelligence activities, from collection, processing, analysis, dissemination of finished intelligence, to the planning and conduct of risky covert operations, require the participation of dozens if not hundreds of cleared personnel, at various levels. Depending on the classification level and compartmentalization of the intelligence involved, the final product could be transmitted via secure computer networks to thousands of individuals with the appropriate security clearances. Therefore, intelligence effectiveness at times demands a high level of involvement of "cleared" personnel. Intelligence is worthless if it does not get to the tactical, operational or strategic decisionmaker in a timely fashion and in a format he or she can understand and act on. However, at the same time, the sheer scope and scale of such an operation increases the risks of unauthorized disclosure. The key question is, from where is the greatest threat of compromise to sensitive intelligence sources and methods?

As stated earlier, espionage by well-placed American intelligence officials has caused the greatest damage to the IC's abilities and effectiveness. Over the past two decades, a number of high profile espionage cases have come to light. In a July 2002 study by Katherine Herbig and Martin F. Wiskof titled, *Espionage Against the United States by American Citizens 1947-2001,* the authors documented 150 cases of espionage against the United States by American citizens between 1947 and 2001.[33] In addition to the CIA's Aldrich Ames (arrested in February 1994) and the FBI's Robert Hansen (February, 2001), there have been dozens of lesser known cases that have also done significant damage to the IC's ability to carry out its mission. Individuals such as the former National Security Agency's (NSA) communications specialist, Ronald W. Pelton, who after quitting his job in 1979, sold valuable secrets to the Soviet Union until his arrest in and conviction in the mid-1980s; former Navy intelligence analyst Jonathan Pollard, who pleaded guilty to spying for Israel in 1986; former Defense Intelligence Agency analyst Ana Montes who worked for the Cuban intelligence service for 16 years, her entire career as a DIA analyst, until her arrest and conviction in 2001-2002, have all caused irreparable damage to American intelligence capabilities by giving Hostile Intelligence Services (HOIS) detailed information on U.S. intelligence "sources and methods" of collection and "gaps" in our collection or analytical capabilities.

A level below espionage is unauthorized "leaks" of classified information to the media. Some, such as the Glomar Explorer example cited above, can have serious financial and intelligence collection consequences. However, many are "leaks" of classified material that have more to do with policy decisions than intelligence "sources and methods." Most of these leaks tend to be a continuation of internal policy debates that have a more limited impact on sensitive intelligence capabilities when compared to the espionage cases mentioned above. As the recent perjury trial of the Vice President's former Chief of Staff, I. Lewis "Scooter" Libby, revealed, there has always been a symbiotic relationship between senior administration policymakers and the major print and broadcast media. During the trial, ten well-known journalists testified that they were provided "sensitive" information by multiple senior administration sources.[34] Veteran journalist and senior *National Public Radio* news analyst, Daniel Schorr, claims there is a dichotomy of intelligence leaks, "the top-level leak serving some administration purpose, and the unauthorized subterranean, whistle-blowing leak that tends to defeat the administration's purpose."[35] The most famous example of the latter is the leak of the so-called *Pentagon Papers* on American involvement in Vietnam in June 1971. Since the documents dealt mostly with American government policy decisions regarding Vietnam over the previous three decades, the impact on intelligence effectiveness was negligible. Schorr thinks both types of leaks, while dangerous, will continue. He notes that "the ship of state is the only kind of ship that leaks mainly from the top."[36]

In addition to actual "leaks," journalists around the world have increasingly stumbled onto sensitive intelligence and covert operations abroad. Depending on their nationality, and media affiliation, they must then decide whether or not to publish their stories, or hold back at the

request of the intelligence agencies involved, or even from senior administration officials. This phenomenon will likely increases as information tools become increasingly available to both established and freelance journalists all networked together in the “blogosphere.”

My purpose for pointing out these various forms of compromise of sensitive intelligence sources and methods is to question the conventional wisdom that Congress is the primary source of intelligence leaks, and therefore not trustworthy enough to perform serious oversight responsibilities on behalf of its constituents as a co-equal branch of government. The evidence to support this harsh accusation is weak. As Lowenthal points out:

Despite these precautions and the internal rules intended to punish members or staff who give out information surreptitiously, Congress as an institution has the reputation of being a fount of leaks. This image is propagated mainly by the executive branch, which believes that it is much more rigorous in handling classified information. In reality, most leaks of intelligence and other national security information come from the executive, not from Congress. (In 1999 DCI Tenet admitted before a congressional committee that the number of leaks from executive officials was higher than at any time in his memory.)

This is not to suggest that Congress has a perfect record on safeguarding intelligence material, but it is far better than that of the CIA, the State or Defense Departments, or the staff of the NSC. The reason is not superior behavior on the part of Congress so much as it is relative levers of power. Leaks occur for a variety of reasons: to show off some special knowledge, to settle scores, or to promote or stop a policy. Other than showing off, members of Congress and their staffs have much better means than leaks to settle scores or affect policy. They control spending, which is the easiest way to create or terminate a policy or program. Even minority numbers and staff can use the legislative process, hearings, and the press to dissent from policies or attempt to slow them down.[37]

Although the history of congressional oversight is limited to several decades, there is little evidence that Congress—especially the Senate Select Committee on Intelligence (SSCI) or the House Permanent Select Committee on Intelligence (HPSCI)—has been a significant source of “leaks” that have compromised sensitive intelligence programs, sources or methods.[38]

While both congressional intelligence oversight committees have been hobbled over the past fifteen years by excessive partisanship, inattention in the post-cold war era, and deference to the executive branch in the conduct of the war on terror, there are strong indications that congressional oversight may soon experience a renaissance. One example is the recent National Intelligence Estimate (or NIE) on Iraq, *Prospects for Iraq’s Stability: A Challenging Road Ahead*, released in late January 2003. One of the most intriguing parts of the unclassified version released by the Office of the Director of National Intelligence (ODNI) was not the document’s assessment on Iraq, but the first four of the eight pages which dealt exclusively with how the NIE process was conducted. The ODNI also acknowledged that the latest Iraq NIE was requested by *Congress*, not the administration. This is highly unusual; the last time Congress made such a request for a National Intelligence Estimate was the 2002 NIE on the threat posed by Iraq’s WMD programs.[39] The new House and Senate leadership are also debating changes to committee responsibilities to consolidate intelligence-related programs and budgetary powers as well as other recommendations made by the 9/11 Commission with regard to their oversight responsibilities.[40]

Finding the Right Balance: Risk Versus Gain

Intelligence, especially quality all-source intelligence, is not only expensive, it takes a very long time to develop, and at times entails significant risks. The intelligence paradox has always been that during times when the threat to U.S. national security seems implausible (post-Cold War

1990s) or remote (pre-9/11 Afghanistan), or both (Germany and Japan during the 1920s and 30s interwar period), is when the nation should be the most aggressive recruiting agents, developing technical collection capabilities and building the analytical expertise needed for a future crisis that may not become urgent for years. Unfortunately, that is often when short-sighted budget-cutters, career bureaucrats and executive and legislative leaders become most risk-averse. It is common for even the most prudent intelligence initiatives to be shelved during this period. Rapid efforts to redress intelligence collection and analytical shortfalls are rarely successful if implemented only after a crisis has developed.

The debate over secrecy and transparency is almost of secondary importance compared to the executive and legislative responsibilities to insure the IC is focused on the right problems, is developing the right tools, recruiting and retaining the right people, and spending the money Congress authorizes and appropriates to various intelligence agencies wisely. The size and scope of the U.S. IC's responsibilities and activities today demand enhanced internal and external executive and congressional oversight, not just to protect the rights and security of its citizens—and the taxpayers' investment—but also to ensure the IC is on the right track in terms of its focus and long-term vision. The American public, and their elective representatives, are entitled to the highest standard of performance from their intelligence professionals given the potential impact of shoddy or politicized intelligence work.

Since Pearl Harbor, over four decades of Cold War, and more recently the War on Terrorism, the United States has begrudgingly accepted the need for a robust, aggressive and permanent intelligence apparatus to protect the nation in an increasingly dangerous world. Ever since World War II, we have struggled with the dilemma of maintaining sufficient secrecy to allow the IC to operate effectively, and at the same time permitting adequate transparency to allow oversight safeguards. The IC's seventeen agencies—which now include the new Office of the new Director for National Intelligence (ODNI)—all posses internal oversight mechanisms such as General Councils or Inspector Generals.

Congress, with a permanent intelligence committee in both the Senate and the House, staffed by experienced professionals, and operating with procedures developed over three decades, can and should play an important intelligence oversight role. According to Lowenthal, the U.S. system is more developed in this area than any other industrialized power.

In democracies, oversight tends to be a responsibility shared by the executive and legislative powers. The oversight issues are generic: budget, responsiveness to policy needs, the quality of analysis, control of operations, propriety of activities. The United States is unique in giving extensive oversight responsibilities and powers to the legislative branch. The parliaments of other nations have committees devoted to intelligence oversight, but none has the same broad oversight powers as Congress.[41]

Yet, a major issue facing the American public with regard to intelligence transparency today is whether Congress is structured properly and has the tools to carry out its wide-ranging intelligence oversight responsibilities in an effective and bipartisan manner?

The Way Ahead

Five and a half years since the 9/11 tragedy, there is little evidence that America's Global War on Terrorism will be ending anytime soon. Like the end of the Korean War, America and its allies are settling in for a prolonged conflict with a global ideological foe that is adaptive, resourceful and ruthless. Some within the Departments of State and Defense are even trying to rename the struggle against this virulent form of radical militant Islam "the Long War" instead of Global War on Terrorism. America and its security institutions will have to adjust accordingly if it is to fight an effective and prolonged Cold War-like struggle that could possible last decades. The emergency

powers contained in the Patriot Act will have to be more closely aligned with the traditional civil liberties and due process Americans expect in their democracy.

Congress will have to abandon its episodic interest in intelligence oversight responsibilities and invest the necessary time and resources to carry out its duty as a co-equal branch of government. The members and staff selected to serve on the HPSCI and SSCI will be confronted by an increasing number of complex intelligence-related issues. It will have to hire the best and most experienced intelligence staffers if it is to be an effective contributor to making sure the U.S. IC is up to the global challenges in the 21st century.[42] This is a tall order given the enormous size and scope of the U.S. IC today, and will require major changes in how Congress conducts its oversight responsibilities.

Like the Intelligence Community, the congressional oversight committees have always faced the dilemma on whether to focus their limited staff and time on short-term issues (budgets, investigations, confirmation hearings, ongoing and emerging crises in certain geographic areas, etc.) vice long-term challenges (restructuring the Cold War-era intelligence agencies for 21st century challenges; the recruitment, training and retention of a quality intelligence workforce; cost-benefit comparative analyses of the various technical collection programs, etc.) As is true within the IC, long-term concerns often lose out to the immediate requirements. To ameliorate this problem, the congressional oversight committees need to establish an organization designed to step back from the daily chores of hearings, investigations and budgetary minutiae and focus on the wider and longer-term intelligence challenges facing the nation over the horizon. Such an organization already exists in the executive branch. The President's Foreign Intelligence Advisory Board (PFIAB) was first created by President Eisenhower in 1953, and has assisted numerous presidents since then. It usually consist of senior intelligence and policy officials, including such luminaries as former National Security Advisor, Brent Scowcroft, former Senator Warren Rudman (R-NH), and former Chairman of the Joint Chiefs of Staff, Admiral William J. Crowe, Jr.

The congressional intelligence oversight committees could benefit from a PFIAB counterpart that could take a longer, wider and deeper view and serve as senior consultants on complex intelligence issues facing the oversight committees' members and staff. Distinguished individuals with exceptional intelligence credentials such as former Senators Sam Nunn (D-GA); Warren Rudman (R-NH); William Cohen (R-ME); and Congressman Lee Hamilton (D-IN) are examples of the type of distinguished individuals who should serve on such a Congressional Foreign Intelligence Advisory Board (CFIAB).[43]

Conclusion

"If doctors bury their mistakes, intelligence officers tend to classify theirs."

—Anonymous

The issues of U.S. IC's accountability, transparency and effectiveness have taken on increased importance following a number of recent failures and an increasingly ominous global security environment. The veil of secrecy covering the nation's intelligence activities will have to be pulled back a bit, for a selected group of trusted legislators, judges and media personnel, to reassure an anxious American public that the IC is focused on the right enemy, has the appropriate resources, and is not trampling the civil liberties of law-abiding citizens as they conduct their important work. Besides the considerable financial costs, the political costs of the American public losing confidence in the competence and professionalism of its intelligence services can have a devastating impact on the morale of IC's estimated 100,000 employees. Many have already left government service for more lucrative, and safer, careers in the private sector. Yet the challenge remains for the executive and legislative branches to develop an effective intelligence system that can anticipate threats, identify opportunities and protect civil liberties. Since those early days of

executive and congressional intelligence cooperation in the War of Independence, the record of effective congressional oversight of the U.S. IC has been brief and uneven at best. Partisan squabbles have seriously hamstrung congressional oversight since the end of the Cold War. Yet cooperation between the executive and legislative branches is possible and remains necessary if we are to build and maintain the intelligence capabilities this nation desperately needs and deserves.

The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.

References

1. In Christopher Andrew*, For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (New York, NY: HarperCollins Publishers, 1995), 8. Also, see "Intelligence in the War of Independence," in the publications section of the CIA website.

2. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, Third Edition (Washington, DC: CQ Press, 2006), 12.

3. *Ibid.*, 12.

4. Much of the information on the U.S. IC, such as the exact number of personnel and budgets remain classified. However, Ambassador Negroponte, in a speech at the National Press Club marking his first year anniversary as the Director of National Intelligence, stated, "the U.S. Intelligence Community comprises almost 100,000 patriotic, talented and hardworking Americans in 16 federal departments and agencies." The previous year, his top deputy for collections, Ms. Mary Margret Graham, announced that the overall U.S. intelligence budget was $44 billion. See Katherine Shrader, "Intelligence Chief Says Personnel Number 100,000," *ABC News*, February 12, 2007. In 1997, Ambassador Negroponte's predecessor, Director of Central Intelligence George Tenant, revealed that overall intelligence spending for fiscal 1998 was $26.6 billion, in a response to a Freedom of Information Act suit. See, Lowenthal, *Ibid.,* 205.

5. General Washington's spies dealt primarily with military intelligence, while the Second Continental Congress focused on strategic diplomatic intrigue. Washington relied heavily on secret intelligence to keep his fledgling army from falling victim to operational or tactical surprise as it did in the catastrophic rout in the battle of Long Island in late August 1776. The Second Continental Congress was keenly aware of America's need for foreign intelligence and foreign alliances. As early as November 29, 1775, the Second Continental Congress began establishing a number of secret committees, by resolution, to aid the war effort through foreign political intelligence. On April 17, 1777, the Committee of Secret Correspondence was renamed the Committee of Foreign Affairs, but kept with its intelligence function. See Christopher Andrew, *Op. Cit.,* 6-12.

6. Andrew, *Ibid.,*13.

7. For an overview of Congressional oversight of the U.S. Intelligence Community from 1947 to the present, see Denis McDonough, Mara Rudman, and Peter Rundlets, "No Mere Oversight: Congressional Oversight of Intelligence is Broken," *Center for American Progress*, 2006.

8. *Ibid.*, 15.

9. Abram N. Shulsky (revised by Gary J. Schmitt), *Silent Warfare: Understanding the World of Intelligence, Third Edition,* (Washington, D.C.: Brassey's, 2002), 172.

10. For more on allied code breaking during World War II, see James Bamford, *The Puzzle Palace* (London: Penguin Books, 1982), and David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes 1939-1943* (New York, NY: Barnes and Noble Books, 1991).

11. Breffni O'Rourke, "Middle East: Fatal Crash Proves the U-2 Spy Plane, While Seldom Seen, Is Still Often Flown," *Radio Free Europe/Radio Liberty*, June 23, 2005.

12. See, Federation of American Scientists Intelligence Research Program, "Project Jennifer Hughes Glomar Explorer." Also, "The Great Submarine Snatch," *Time Magazine*, March 31, 1975.

13. Pete Earley, "Treason" (from *Confessions of a Spy*), *U.S. News and World Report*, February 17, 1997, 28-35.

14. Ben Fenton, "FBI Spy Who Sold Out to Russia 'Did Megaton Damage'," *The Telegraph*, June 19, 2001.

15. James Fallows, "Spy's Eye View: Google Earth and its rival programs offer (Civilians) a new way to look at the world," *The Atlantic Monthly*, March 2006, 142.

16. Zoe Mutter, "Terrorists Tap into Google Earth: Free Maps Used to Pinpoint British Troops," *PC Advisor,* January 16, 2007.

17. "Vernon A. Walters Quotes," *BrainyQuote.com*.

18. Dan Eggen, "66% Think U.S. Spies on its Citizens," *Washington Post*, December 13, 2006, 19.

19. *Ibid.*, 19.

20. See *The 9/11 Commission Report* of the National Commission on Terrorist Attacks Upon the United States, Washington, DC. 2004.

21. See the *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005.

22. See the U.S. Department of Defense, Office of the Assistant Secretary of Defense (Public Affairs) News Transcript, "Briefing on the Iraq Survey Group," May 30, 2003, and the *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD*, September 30, 2004.

23. See the *Iraq Study Group Report*, 93-96, December 6, 2006.

24. *Ibid.*, 95-96.

25. See, Lowenthal, *Op. Cit.,* 205.

26. See National Aeronautics and Space Administration's *FY 2008 Budget Estimates.*

27. Elana Schor, "Wilkes and Foggo Indicted," *The Hill*, February 14, 2007, and Brian Ross, "Foggo Indictment Expected: Dark Day for the CIA," *ABC News,* February 13, 2007.

28. Walter Pincus, "Many In Government Helped Cunningham Or Yielded, Panel Finds," *The Washington Post*, October 18, 2006, 19.

29. *Ibid.*

30. *Ibid.*

31. Walter Pincus, “Pentagon Expanding Its Domestic Surveillance Activity,” *The Washington Post*, November 27, 2005, A06.

32. *Ibid.*

33. Katherine Herbig and Martin F. Wiskof, *Espionage Against the United States by American Citizens 1947-2001,* TRW Systems, July 2002.

34. Michael J. Sniffen, Associated Press writer*,* “Journalists Name Additional Leak Sources,” *Boston.com*, February 12, 2007.

35. Daniel Schorr, “The Dichotomy of Intelligence Leaks,” *Christian Science Monitor*, February 17, 2006.

36. *Ibid.*

37. Lowenthal, *Op. Cit.,* 204-205.

38. See Marvin C. Ott, “Partisanship and the Decline of Intelligence Oversight,” *International Journal of Intelligence and Counterintelligence* 16, No. 1 (Winter 2003), in Roger Z. George and Robert D. Kline, eds. *Intelligence and the National Security Strategist: Enduring Issues and Challenges* (Washington, D.C.: National Defense University Press, 2004), 103-123.

39. See the Office of the Director of National Intelligence, National Intelligence Estimate, “Prospects for Iraq’s Stability: A Challenging Road Ahead,” January 2003.

40. “Intelligence Oversight in the New U.S. Congress,” *Jane’s Defense Weekly*, January 19, 2007.

41. Lowenthal, *Op. Cit.*, 191.

42. In the fall of 2006, reporter Jeff Stein interviewed various members of the House and Senate Intelligence Oversight Committees and ended each interview with the straightforward and fundamental question. “Do you know the difference between a Sunni and a Shiite?” His rationale was that British Intelligence, and the government and parliamentary officials they report to, would have a fairly good understanding of Protestant and Catholic factions in Northern Ireland. Stein was surprised, and somewhat alarmed, to learn many senior members had no idea what the differences were, or which branch al-Qaeda’s leaders followed. “…as I keep asking it around Capitol Hill and the agencies, I get more and more blank stares. Too many officials in charge of the war on terrorism just don’t care to learn much, if anything, about the enemy we’re fighting.” see Jeff Stein, “Can You Tell a Sunni From a Shiite?” *New York Times*, October 17, 2006.

43. For a description of the PFIAB and it oversight responsibilities, see “United States Intelligence Community, Oversight and Guidance, Relationships with other Government Organizations,” *Intelligence.gov*, the official website of the U.S. IC.