The NCIX and the National Counterintelligence Mission: What has Worked, What has Not, and Why

INTRODUCTION:

Foreign intelligence services have stolen U.S. national security secrets for decades. The damage Aldrich Ames, Robert Hanssen, and Chinese agents have inflicted on U.S. national security has been incalculable. To remedy this problem, the office of the National Counterintelligence Executive (NCIX) was established in 2001 to provide strategic direction to U.S. counterintelligence (CI) and to integrate and coordinate the diverse CI activities of the U.S. government (USG). Nevertheless, interagency struggles and a lack of authority have frustrated the new office. American secrets remain excessively vulnerable to foreign intelligence services.

This case study, written by the first National Counterintelligence Executive appointed by the President, discusses the challenges of leading and integrating the U.S. CI enterprise. It discusses issues ranging from the practical details of setting up and staffing a new USG office to the interagency mechanisms for reaching consensus and implementing policy. The study also explains the significance of the first national counterintelligence strategy, which established new policy imperatives to integrate CI insights into national security planning and engage CI collection and operations as a tool to advance national security objectives.

STRATEGY:

U.S. counterintelligence duties have historically been dispersed among independent departments and agencies. By creating the NCIX, the Congress sought to replace this divided approach with a more integrated and effective U.S. CI apparatus. The Counterintelligence Enhancement Act established the duties of the NCIX, which include: identifying and prioritizing the foreign intelligence threats of concern to the United States; developing a strategy to guide CI plans and programs to defeat those threats; evaluating the performance of the CI agencies against those strategic objectives; and ensuring that the budgets of the many CI organizations of the federal government are developed in accordance with strategic priorities. In 2005, the NCIX issued the first *National Counterintelligence Strategy*, which set forth consistent, clear, and new strategic direction for U.S. counterintelligence. The subsequent creation of the office of the Director of National Intelligence, to whom the NCIX now reports, consolidated the NCIX mission within the new architecture of U.S. intelligence.

INTEGRATED ELEMENTS OF NATIONAL POWER:

Getting the departments and agencies to work together with the NCIX to implement the national CI strategy has proven an elusive goal. Efforts towards this end have been complicated by the unique history of the disaggregated U.S. CI enterprise, deficiencies in the NCIX and DNI organizations, and a seeming lack of awareness of the gravity of foreign intelligence threats among national security leadership. Interagency cooperation in many cases proved anathema to the U.S. government's CI organizations. The FBI, for example, which consumes the lion's share of U.S. CI dollars and billets, unilaterally withdrew most of its personnel from the NCIX office. In addition, the FBI's counterintelligence division published its own "national strategy for counterintelligence" two months after the NCIX's

presidentially approved strategy was issued. The creation of the DNI did not facilitate cooperation––in fact, the DNI has worked to weaken the NCIX as it has eclipsed that office's authorities in counterintelligence budget, collection, and coordination.

EVALUATION:

The Counterintelligence Enhancement Act established a national leader to bring strategic direction to U.S. counterintelligence, but the legislation failed to establish a strategic counterintelligence *program*. While charging the NCIX with responsibility for heading counterintelligence, the law did not assign the NCIX the authorities needed to manage a strategic CI program. Though the NCIX office is responsible for providing strategic direction to U.S. counterintelligence, it does not have the power to direct budget allocations. Program and budget authorities for CI activities remain divided among the departments and agencies and subject to their individual priorities, which too often take precedence over national objectives.

Similarly, NCIX is given the responsibility to evaluate department and agency performance, but it is not empowered to direct programmatic changes. Under this model, the NCIX is inherently advisory, rather than authoritative. In addition, within the office of the DNI, authorities and lines of responsibility for counterintelligence have become blurred, diluting the concentrated focus and guidance that the NCIX was created to provide.

RESULTS:

A series of government and independent analyses have documented the high costs of the seams in U.S. counterintelligence strategy. Failing to establish an effective national CI leader threatens to replicate past costs. Seven years after the NCIX was created, no single entity is capable of providing a comprehensive threat assessment of possible foreign intelligence successes, supporting operations, or formulating policy options for the President and his national security team. While CI-related cooperation among the FBI, CIA, and the military services has increased, this collaboration has failed to provide the comprehensive, well-integrated CI strategy and policies required to uphold U.S. national security.

CONCLUSION:

The NCIX seemed poised to succeed when created. It had widespread congressional support, a consolidated National Strategy, the endorsement of a highly respected commission, and the President's personal backing. Yet, the statutory intent to integrate U.S. CI efforts has been repeatedly frustrated. Due to the weaknesses of the NCIX and the lack of a strategic program, individual agency priorities have eclipsed USG-wide CI integration. As a consequence, Washington has inadequately addressed the threats posed by foreign intelligence agencies to U.S. national security.

FOREWORD BY James R. Locher III
Executive Director, Project on National Security Reform

PROJECT ON NATIONAL SECURITY REFORM

CASE STUDIES VOLUME I

RICHARD WEITZ, EDITOR

TRANSFORMING GOVERNMENT
FOR THE 21ST CENTURY

CHAPTER 2. THE NCIX AND THE NATIONAL COUNTERINTELLIGENCE MISSION: WHAT HAS WORKED, WHAT HAS NOT, AND WHY

Michelle Van Cleave[75]

Introduction and Overview

The Project on National Security Reform, and the series of case studies that inform it, center on four key questions:

- Can the U.S. government integrate elements of national power in theory (i.e., develop real strategies)?
- If so, can it then implement them (get the agencies/departments to work together)?
- If not, what explains such failure (in general terms)?
- How much does that failure cost us?

When I first saw these questions, I was struck by how closely they paralleled my concerns during the two and a half years I served as the first statutory head of U.S. counterintelligence.

The national counterintelligence executive (NCIX) was first established in 2001 to provide strategic direction to U.S. counterintelligence (CI), and to integrate and coordinate the diverse CI activities of the government. Its statutory mandate is clear, including carefully enumerated functions and an interagency mechanism to enable coordination of the many CI organizations across the executive branch. The subsequent creation of the office of the Director of National Intelligence, to whom the NCIX now reports, consolidates the NCIX mission within the new architecture of U.S. intelligence.[76]

---

75 Former National Counterintelligence Executive (2003–2006). The views expressed in this paper are those of the author alone and do not necessarily reflect the views of the Director of National Intelligence or any other part of the U.S. Government.

76 The office of the NCIX is one of three major centers under the Director of National Intelligence; the other two are the National Counterterrorism Center

Yet the statutory intent has been frustrated at every turn. Strategic integration takes a back seat to individual agency priorities. National leadership exists in name only. Across the government, our CI capabilities are in decay. We seemingly cannot get ahead of the cycle of losing talent. And the potential costs of failure are profound.

This case study examines the historical context behind the establishment of the National Counterintelligence Executive, reflecting the unanimous judgment of the president, the Congress, an interagency study, and a Presidential Commission on the need to transform the nation's CI enterprise. It contrasts the legacy business model of U.S. counterintelligence, in which tactical CI duties are dispersed among independent departments and agencies, with the concept and mission of defeating foreign intelligence threats as an integral instrument of national security strategy. The challenges of leading and integrating the U.S. CI enterprise are discussed, from the practical details of setting up and staffing a new government office to the interagency mechanisms for reaching policy decisions and implementing national strategic direction. And it explains the significance of the nation's first national counterintelligence strategy, which established new policy imperatives to integrate CI insights into national security planning, to engage CI collection and operations as a tool to advance national security objectives, and, at the strategic level, to go on the offense.

This story opens on a high note. It would be difficult to find a clearer expression of national strategic guidance than the combination we enjoyed of congressional support, a consolidated National Strategy, the consistent findings of a highly respected commission, the president's embrace of its recommendations, and a running score card on their implementation. By any measure, during my time in office, the statutory NCIX mission to lead and integrate U.S. counterintelligence was well positioned to succeed.

Nevertheless, that clarity of purpose proved insufficient to navigate the well-entrenched institutional obstacle course. As this case study will show:

---

and the National Counterproliferation Center.

The law creating the NCIX fell short of the mark. It established a new head for counterintelligence, but carefully denied the NCIX any directive authority. It created a national executive to provide strategic focus, but not the means of execution. Guidance from such an executive is inherently advisory, rather than authoritative. To achieve strategic coherence, U.S. counterintelligence does not need an advisor, it needs a leader. And the nation needs a clearly defined strategic CI program to defeat foreign intelligence threats, with the dedicated resources, authorities, and accountability that implies. The statutory scheme omitted these essential elements, which severely undercut the effectiveness of the NCIX and the national CI mission.

The new intelligence architecture under the Director of National Intelligence (DNI) has become part of the problem. Within the office of the DNI, authorities and lines of responsibility for counterintelligence are blurred, diluting the concentrated focus and guidance that the NCIX was created to provide. Without clear and effective central leadership, the several CI components naturally look first to their legacy responsibilities rather than the new challenges that the NCIX-led strategic reorientation of the nation's CI enterprise would impose. To be sure, even a fully empowered NCIX would not be sufficient to transform U.S. counterintelligence: the centrifugal forces protecting legacy divisions of responsibility and other impediments to national integration are and would remain formidable. But many of the difficulties we encountered in moving the CI enterprise to carry out the strategic CI mission would have been significantly lessened.

There is a debilitating gap between the national security decision-making process and the work of U.S. counterintelligence. It is up to the president and his policy leadership to judge the importance to U.S. national security of countering foreign intelligence operations and to issue policy guidance based on those judgments. But first they need to be presented with the essential insights into foreign intelligence plans, intentions and capabilities, to be able to assess their impact on U.S. national security, which presents somewhat of a chicken-and-egg problem. The intelligence community will not turn its resources to collect and analyze foreign intelligence activities as an input to inform policy makers unless so tasked; but with little to no insights into foreign

intelligence activities, there is nothing to alert the policy maker to the threats they present. The modalities for coupling national security policy direction to strategic CI output are not difficult to devise, but they have yet to be institutionalized.

As a consequence, the U.S. government has been slow to appreciate the effects of foreign intelligence operations, much less to address the threats they pose to current U.S. foreign policy objectives or enduring national security interests. We know surprisingly little about adversary foreign intelligence services relative to the harm they can do, or relative to the insights to be gained by analyzing the distinctive ways in which they operate, and the different purposes they serve. U.S. capabilities to disrupt, degrade, or exploit the intelligence operations of potential adversaries remain woefully inadequate to answer that call. And the national counterintelligence mission is quietly on hold.

I offer this case study of the NCIX and the national counterintelligence mission in the hope that it might contribute to the larger purposes of the Project on National Security Reform. I invite readers to consider the broader, related question of how U.S. efforts to counter foreign intelligence threats can and should be integrated with other instruments of state power. This case study is also offered in the hope that the next NCIX and our national security leadership will be able to learn from past shortcomings (including my own), to the betterment of our Nation's counterintelligence enterprise and the vital strategic mission that counterintelligence alone can perform.

The Historical Context

Washington was still in transition mode between administrations, arguing about last-minute pardons and missing "W" computer keys,[77] when the new attorney general called a press conference. Robert

77 John F. Harris and Dana Milbank, "At the White House, 'Moving On' or Piling On?; Bush and GOP Gain, Democrats Blush, and Ex-President's Allies Cry Foul Over Tales of Messy Exit," *The Washington Post*, (Washington, D.C.: Feb 18, 2001) A.10. Among those pardoned was former DCI John Deutsch for his criminal hubris in storing a staggering quantity of the nation's most sensitive secrets on his home computer and unclassified laptops—the electronic

Hanssen, a senior Federal Bureau of Investigation (FBI) special agent, had been arrested for espionage. For more than two decades, Hanssen had established a reputation as a competent, forward-leaning member of the bureau's counterintelligence division, a trusted insider in all FBI operations run against the Soviet Union and in other national programs of extreme sensitivity. And for most of those two decades, Hanssen had been spying against his own country, supplying the Russians a wellspring of America's most closely guarded secrets. The damage to U.S. national security was incalculable.

Hanssen is now in jail, a status he shares with another traitor and spy, Aldrich Ames. Ames, a former Central Intelligence Agency (CIA) officer and chief of the Counterintelligence Branch in the Soviet Division of the Directorate of Operations, spent eight years selling secrets to the Russians that went to the heart of U.S. technical and human intelligence collection, resulting in wide-ranging and continuing damage to U.S. national security and the deaths of at least nine clandestine agents. The U.S. intelligence community and especially CIA were shaken to the core by revelations of his treachery.

The Ames case, cemented by Hanssen and preceded by decades of damaging espionage against the United States, revealed a pattern of costly failures in America's struggling counterintelligence enterprise.[78]

Historically, CI responsibilities and authorities in the United States have been divided among the several operational CI entities—the FBI, CIA, and the three military services—with no central leadership or structure to unite them. Not surprisingly, this disjointed architecture

---

equivalent of pasting them on billboards across the globe. In order to read the tightly held damage assessment, I had to sign a sweeping confidentiality agreement covering top-secret compartments and codewords I never knew existed, but with which our adversaries are doubtless well acquainted, thanks to Mr. Deutsch.

78 See database of some 150 U.S. persons prosecuted for espionage or related offenses, compiled by the Department of Defense: "Espionage Cases 1975-2001" Defense Personnel Security Research Center (Monterey, California: GPO, 2002). The records were transferred to the Defense Human Resources Activity, Office of the Secretary of Defense, in December 2002, and designated DHRA 01, entitled "PERSEREC Database." See also their update in Technical Report 08-05 (March 2008), "Changes in Espionage by Americans: 1947-2007."

made it impossible to devise, much less execute, a coherent national counterintelligence strategy to defeat foreign intelligence threats. It also created inherent seams that our adversaries proved both willing and able to exploit.

Most Americans would be astonished by the extent to which foreign intelligence services have been able to steal our nation's national security secrets, often with impunity. With the possible exception of the Coast Guard, every department and agency with sensitive national security responsibilities has been penetrated by hostile intelligence services, most more than once. The former Soviet Union was especially successful in stealing U.S. secrets, a tradition that continues unabated under Vladimir Putin's Russia.[79] (The Russian intelligence presence in the United States is now equal to its Cold War levels, a sizing decision presumably indicative of the return on investment.) But the Russians are far from alone, especially as other hostile services have literally gone to school on the practices of the old KGB. And then there is China. As reported a decade ago by a special Congressional Commission, the Chinese stole the design secrets to all—*all*—U.S. nuclear weapons, enabling them to leapfrog generations of technology development and putting this last line of U.S. defenses at risk.[80] To this day, we do not know how China acquired those volumes of supremely guarded national security information; but we do know that Chinese intelligence is still at work, aggressively targeting not only America's defense secrets but our industry's valuable proprietary information as well.

The lessons of past CI failures were clear. The United States needed a national leader to provide strategic direction to U.S. counterintelligence, and to integrate and coordinate the government's diverse activities to counter foreign intelligence operations of

79 A compelling perspective on contemporary Russian intelligence operations in the United States—and to a lesser extent, U.S. naiveté—can be found in Pete Early, *Comrade J: The Untold Story of Russia's Master Spy in America After the End of the Cold War* (New York: Putnam's Sons 2008). As summed up on book's the front cover: "When the Soviet Union disappeared, the spies did not."

80 Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China ("Cox Commission"), 105th Congress, 2nd session, 1999; Report 105–851.

concern. This was the principal finding of an interagency study, "CI-21," which found its way to the president's desk in late December 2000.[81] As one of his final acts in office, President Clinton signed a Presidential Decision Directive (PDD-75) establishing the National Counterintelligence Executive. The NCIX, as the job would become known, was charged with the mission of bringing coherence to U.S. counterintelligence. Robert Hanssen's arrest less than two months later made the task of the yet-to-be-named NCIX all the more compelling.

At the start of the Bush Administration, all the stars were in alignment for a rebirth of U.S. counterintelligence under a new architecture to enable national coherence and strategic focus. But history had some surprises in store. The director of the FBI selected a senior FBI supervisory special agent to set up the new NCIX office, who was just getting started when September 11 radically reordered the nation's priorities. In short order, he was recalled to FBI headquarters along with most of the other FBI detailees to the fledgling NCIX office, leaving behind a handful of people in temporary quarters wondering what would happen next. PDD-75 was still in force, but there was no NCIX, and it was uncertain what the new administration would do: extend PDD-75, rescind it, or change it in some way? And then Congress decided to intervene.

The Counterintelligence Enhancement Act of 2002 codified the office of the NCIX and elevated the position of NCIX to a Presidential appointment, reporting to the president. Here was an opportunity to lead a great community of dedicated people, on a mission of highest importance to our Nation's security: a privilege—and a challenge—difficult to surpass. Upon the recommendation of the attorney general, the secretary of defense, and the director of central intelligence (DCI), the president appointed me national counterintelligence executive, and in July of 2003, we turned to the business of standing up an office to execute the new national CI mission as set forth in law.

81 CI-21 was not the first effort to reform U.S. counterintelligence. Following Ames' arrest, the DCI established a National Counterintelligence Center to help coordinate CI activities. Its relatively junior status and lack of any authority over execution led CI-21 members to propose a new model, the NCIX.

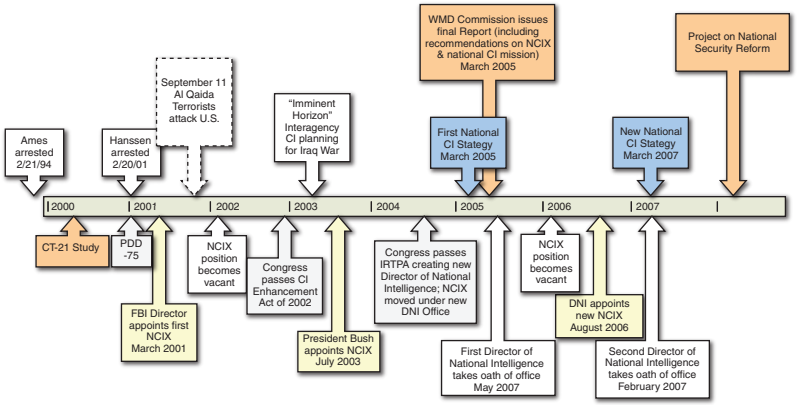

Figure 1: National CI Case Study Timeline

But within a year of my appointment, U.S. intelligence—already reeling from the shock of 9/11—came under intense scrutiny in the wake of intelligence mis-estimates of Iraqi weapons of mass destruction (WMD) capabilities. The ensuing upheaval set the stage for the creation of the DNI, and a bow-wave of change swept over the U.S. intelligence community, catching the newly reconstituted Office of the NCIX in the undertow. Our nascent efforts to transform U.S. counterintelligence came under review and revision, the mission's focus and significance eclipsed by new priorities as the new DNI organization began to take shape.

As of this writing, the plans, processes, and programs to execute strategic CI operations are not in place, and the NCIX office, which was moved under the DNI, has become little more than a fig leaf hiding the decay of our nation's CI capabilities. History may well record that the time was not ripe for effective reform of U.S. counterintelligence. Surely urgency and attention to CI concerns have been lost against the backdrop of the war on Islamic terrorists and the sweeping and still highly unsettled changes in U.S. intelligence writ large.

But there is more to the story than that.

National Mission and Objectives: The National Counterintelligence Mission

Past intelligence failures have inspired a host of proposals for organizational reform. As one scholar observed:

The most frequently noted sources of breakdowns in intelligence lie in the process of amassing timely data, communicating the data to decision makers, and impressing the latter with the validity or relevance of the information. This view of the problem leaves room for optimism because it implies that procedural fixes can eliminate error. For this reason, official postmortems of intelligence blunders always produce recommendations for reorganization and changes in operating norms.[82]

The recent creation of the office of the Director of National Intelligence, successor to the Director of Central Intelligence, is a prime example of this optimism at work.[83]

By sharp contrast, despite a history of damaging CI failures, counterintelligence has been largely immune from reorganization schemes because it never had a conscious organization plan to begin with. The various independent CI elements have grown out of individual department or agency responsibilities, each with its separate jurisdiction and purpose. Unlike the larger intelligence community, with its 60-year history under a DCI, the CI organizations of the

82 Richard Betts, *Enemies of Intelligence* (New York: Columbia University Press 2007) 39, 264

83 While legislation to establish the DNI was pending before Congress, I met with the head of Britain's MI-5, who asked me about the ongoing debate in Washington over how to improve U.S. intelligence capabilities. As we were saying our good-byes, she handed me the following passage:
We trained hard but it seemed that every time we were beginning to form up in teams we would be reorganised. I was to learn later in life that we tend to meet any new situation by reorganising, and a wonderful method it can be for creating the illusion of progress while producing confusion, inefficiency and demoralisation.
The quote was attributed to the Roman statesman Terentius, but I later learned the more likely author was some anonymous disgruntled British soldier during World War II, which only serves to illustrate the universality of the experience and sentiment.

U.S. government had no central leadership and no structure or institutionalized processes to accomplish a central national mission.

The National Security Act of 1947, which established the foundations of the intelligence community, did not assign the national strategic mission of protecting the United States against foreign intelligence threats to the DCI[84] or to any other cabinet secretary or other agency. Yet if asked, I think most national security practitioners would say that they regard counterintelligence as a subordinate discipline to intelligence, and therefore inherently a part of the DCI's responsibilities. And in important respects it is.

But the job of defeating foreign intelligence threats is very different from the job of supplying intelligence to U.S. decision makers. Foreign intelligence operations are directed against a wide array of U.S. national security secrets and operations. Some of those targets are U.S. intelligence activities, and to the extent that CI safeguards the integrity and success of U.S. intelligence, it is an intelligence mission. But foreign powers also direct intelligence operations against other U.S. national security activities and objectives, including proprietary information and technology of commercial value (see Figure 2). What to do about these strategic threats is not an intelligence question; it is a policy call.

The mission of counterintelligence is to identify, assess, neutralize, and exploit foreign intelligence activities directed against the United States and its interests worldwide. Its tactical applications in protecting intelligence collection and other operations are well understood, and executed by the several CI organizations within their spheres of responsibility. This important job is essential to the integrity of U.S. intelligence and the protection of national security information and operations.

84 The DCI's statutory duties were to provide national intelligence, to serve as the head of the intelligence community and the head of the CIA, and to "perform such other functions and duties related to intelligence affecting the national security as the President or the National Security Council may direct." Pointedly the act provides that the terms "'national intelligence' and 'intelligence relating to the national security'… do not refer to counterintelligence or law enforcement activities conducted by the Federal Bureau of Investigation…". National Security Act of 1947, Sec. 103 (50 U.S.C. 403-3)

But foreign intelligence adversaries do not target an individual FBI field office, or a military unit, or a CIA station abroad as an end in itself; they target the United States. In other words, the threat is strategic. Understanding this fundamental point is the first step in a long evolution from thinking about counterintelligence in its several tactical roles to the strategic vision that sees the job of countering foreign intelligence threats as an integral part of achieving national security objectives.

Viewed in this light, counterintelligence is the national security function that supplies insights into foreign intelligence threats to the United States, including options to defeat them as national policy may direct. And its importance is growing.

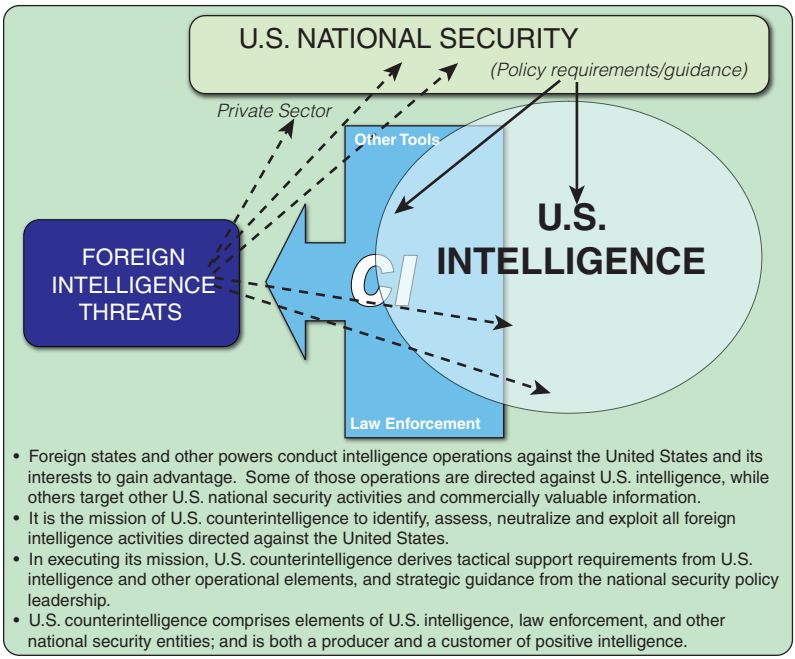

Figure 2: Counterintelligence, Intelligence, and National Security

The growth and pervasiveness of hostile intelligence operations is a striking and largely unappreciated feature of the modern international security environment. Foreign adversaries including the Russians, the

Chinese, the Iranians, the North Koreans, and many, many others use intelligence as an effective instrument of asymmetric power to advance their strategic objectives, exploiting U.S. vulnerabilities to their collection and other intelligence activities. And we are only beginning to appreciate their importance as an extension of state power.

Intelligence operations against the United States are now more diffuse, more aggressive, more technologically sophisticated, and potentially more successful than ever before. In recent years we have seen increasing intelligence operations within our borders facilitated by an extensive foreign presence that provides cover for intelligence services and their agents. Traditional foes, building on past successes, are continuing their efforts to penetrate the U.S. government, while waves of computer intrusions into sensitive U.S. government information systems have confounded efforts to identify their source. We have also seen apparent attempts by foreign partners to exploit cooperative endeavors against terrorist groups to learn essential secrets about U.S. intelligence and military operations, along with an emerging "market" in U.S. national security secrets, which among other things enables foreign practices of deception and denial to impair U.S. intelligence collection. And perhaps most troubling, growing foreign capabilities to conduct influence and other covert operations threaten to undermine U.S. allies and national security interests.

Yet, despite the strategic nature of these foreign intelligence threats, the history of U.S. counterintelligence has been one of dividing responsibilities among several departments and agencies rather than dealing with the strategic whole. Unlike most other states, the United States has never had a unified organization or a national counterintelligence "service" to carry out CI operations. Instead, CI operational authority has been split in gross terms between the needs of domestic security against foreign agents (assigned to the FBI), and the operational needs of human intelligence collection (assigned to CIA) and military actions in the field.[85]

85 In addition to the operational elements (FBI, CIA, and the three military services), other departments and agencies that are particular targets of foreign interest have set up CI offices to meet their individual needs for analytic support or to address insider threat concerns. Key examples include the CI offices within the Department of Energy and its national laboratories; the CI offices within

As a result, U.S. counterintelligence is an amalgamation of specialized activities, each of which is measured on its own terms, rather than for its contributions to a larger whole. The measures of effectiveness in counterintelligence and in personal advancement in the profession have been delimited by individual cases. Did we catch the spy? Did we find the microphones embedded in the embassy walls? Did we discover the true owners of the front company engaged in technology diversion? Such successes are very good things, which can make for fabulous stories revealing flashes of brilliance, creativity and daring, and some true legends in the business.

Far more rare is the case when the operational possibilities of ongoing investigations, or the access of a given penetration, or a double agent tasking, have been fitted against a larger tapestry of the adversary's strategic purpose to inform a CI plan for dealing with the whole. The system is not designed to work that way, for which we pay a hidden cost that becomes all too apparent after the fact in official damage assessments of espionage and other national security compromises. To read through the file drawers cataloging the enormous loss in lives, treasure, and pivotal secrets occasioned by spies and other foreign intelligence coups against the United States is a cold awakening to what is at stake.

The problem is straightforward. The U.S. CI enterprise has not been structured to serve a strategic purpose, nor is it postured globally to disrupt a foreign intelligence service. There is no standard approach to targeting across the CI enterprise; interagency information sharing is poor, and infrastructure support even worse. Even the modest national mechanisms developed to deconflict offensive CI activities stop at the water's edge, a legacy of the old divide between foreign and domestic operational realms. And apart from wartime, we have not routinely addressed foreign intelligence capabilities as part of

---

the several intelligence agencies (e.g., the Natoinal Reconnaissance Office, the National Security Agency, the National Geospatial Intelligency Agency, etc), and other departments with intelligence missions (Treasury Department, the State Department); a number of Department of Defense entities engaged in classified R&D (e.g., the Defense Threat Reduction Agency, the Ballistic Missile Defense Office); and the important CI support functions at the Department of Homeland Security including the U.S. Coast Guard.

a national security threat calculus informing national strategy and planning. As a consequence, the sum of the U.S. CI enterprise is less than its parts could deliver if they were wired to work together as a strategically integrated whole.

"CI-21" and the Counterintelligence Enhancement Act of 2002 represented a conceptual breakthrough in American counterintelligence. They judged that the central strategic core that is needed to identify, assess, and defeat foreign intelligence threats to the United States and its vital interests has been missing. This is the fundamental flaw in the architecture of U.S. counterintelligence that the office of the NCIX was created to remedy, not by its mere existence, but by leading the transformation and strategic integration of our nation's CI capabilities to support national security objectives.

Far from imposing a new layer of bureaucracy, the 2002 reform legislation charges U.S. counterintelligence with executing a new strategic mission that cannot be performed by independent entities acting without central direction or common purpose. The new mission does not peel away authority or responsibility from the several operational organs; rather it levies additional duties on each of them to meet strategic CI objectives. Nor should the new architecture be seen as an indictment of America's CI professionals, who have made tremendous contributions to the security of our nation. Thanks to their dedicated work there is no reason to doubt that we are deriving about as much value as is possible from the old business model of U.S. counterintelligence. But the sum of what our CI agencies do will not bring us a strategic offensive gain against foreign intelligence threats unless orchestrated to a common purpose.

This essential orchestration is the new and force-multiplying job of the NCIX.

Establishing the Office of the NCIX

The Counterintelligence Enhancement Act lays out the duties of the office of the NCIX, in what amounts to a thoughtful enumeration of the functions essential to bringing coherence to disparate CI activities. It directs that the NCIX:

Identify and prioritize the foreign intelligence threats of concern to the United States.

- Develop a strategy to guide CI plans and programs to defeat those threats, and identify the new plans and processes (including R&D) needed to implement that strategy.
- Evaluate the performance of the CI agencies against those strategic objectives.
- Oversee and coordinate the production of strategic analyses of foreign intelligence capabilities, and establish priorities to guide collection and operations.
- Ensure that the budgets of the many CI organizations of the federal government are developed in accordance with strategic priorities.
- Ensure that the workforce has the training and education necessary to meet professional standards and the needs of the strategic CI enterprise.
- And finally—unusual for an intelligence organization—carry out and coordinate outreach programs to advise other government entities and the public about foreign intelligence threats.[86]

Describing these functions is comparatively straightforward. The difficult part comes in determining how to perform them (especially given the limited grant of necessary authority, as discussed herein). The "how to" embraces mastering the complex subject matter that is counterintelligence, what a classic treatise called "an intellectual challenge of almost mathematical complexity."[87] Perhaps almost as challenging are the questions of how the highly diverse organizations, programs, processes, traditions, and egos that make up the U.S. counterintelligence community can be marshaled to achieve strategic

86 50 USC 901. The Counterintelligence Enhancement Act of 2002 was carried forward into the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, December 17, 2004 (50 USC 401), which created the DNI.

87 Christopher Felix, *A Short Course in the Secret War*, 4th ed. (Lanham, Maryland: Madison Books, 2001), 123.

ends; and how to identify and fill in the missing elements, starting with the roles and missions of the new office of the NCIX.

It may seem straightforward, but the question of how the new office of the NCIX should be organized, resourced, and directed invites different answers, depending on one's vision for the mature organization. What is its core purpose, focus, key functions, lead customers, and unique resource needs? Answering these questions is the starting point for standing up any new government office (or as Yogi Berra said, "If you don't know where you're going, you're likely to end up somewhere else"). I developed and evaluated several alternatives for building the office of the NCIX (see summary matrix in Appendix A), before adopting the business model that came to define the value added I expected from the new office and its place in the U.S. CI architecture. Actually putting the nuts and bolts in place proved more difficult.

When I reported for duty, I inherited a staff of about 40 people—a combination of contractors and government personnel on detail from the FBI, CIA, and Department of Defense (DOD)—working out of a suite of tired offices in an undisclosed location somewhere in Northern Virginia. There was no manual or historical precedent to define the business of the office, so the staff largely had been operating on autopilot (which among other problems had resulted in a tangle of ill-fitting contracts and other management headaches requiring corrective action). My first job was to define *their* jobs: to lay out what I expected of each of them individually, what we together needed to achieve, what our measures of success would be… and to build a team perspective among a collection of detailees who were wary of jeopardizing future assignments back to their home agencies.

The succinct assigned mission of the NCIX is to head U.S. counterintelligence – something that had never been done before. But first, we had to set up an office with the attendant practical requirements of securing a lease, building the necessary physical, information technology (IT) and legal infrastructures, establishing human resources and contracting systems, and so forth – all of which had been done before. Or so I thought.

But the stand-alone office of the NCIX was a square peg in the round hole of the CIA administrative structure, which existed first to meet

agency needs, second to meet the community needs of the DCI, and last (as provided under the Counterintelligence Enhancement Act) to support the new office of the NCIX. The coming months would reveal the time-consuming complexities of such seemingly minor challenges as hiring staff (the law made the NCIX office an independent organization drawing administrative support from CIA but pointedly not a part of CIA – very confusing for the personnel system), and getting the lawyers to agree on a number of questions of seeming first impression, e.g., how to exercise statutorily conferred independent authority to enter into contracts.

For the administrative support system, anything that is different is a problem at least initially, because it does not fit into the known set of rules and procedures. This effect is multiplied when the objective is to wire together disparate security regimes governing computer systems, personnel practices, and physical space.[88] We did not know it at the time, but the effort invested in sorting through this maze of law and regulation and practice would help pave the way for the later establishment of the office of the DNI, which would have to address many of the same problems on a larger scale.

We identified centrally located office space, engaged builders and IT support, bought new furniture and carpets and signage, and finally packed up our worldly goods (including some of the most sensitive records the U.S. government possesses) to establish our new headquarters in Crystal City in time for the Fourth of July 2004. And not a moment too soon: the week after we moved out, the roof collapsed.

88 The long pole in the tent in setting up the new office was importing several independent IT systems, with varying rules governing access and physical protection, which had to co-exist in secure space. Given the extreme sensitivity of the work of the NCIX, we were scrupulous in meeting (and even championing) security practices; but also keenly appreciated the daily cost of the lack of interoperability among the IT systems employed by different intelligence agencies. Recognizing that building a CI "community" could not happen without a common communications network, we funded, developed, and deployed such a network for CI users … but when I left office it was still little more than an extra e-mail in-box to check in the morning, rather than the backbone communications system we had hoped it would become.

One of the enduring problems we encountered was in recruiting capable personnel to work in the new CI office. All national "centers" have an inherent personnel problem: you want and need the best and the brightest, but there are never enough of those to go around. The national office draws its staff from the several departments and agencies, who in turn want to keep the most talented personnel in place. Even if a given individual is personally disposed to take an assignment with the national office, getting their line management's okay is far from easy. ("No. You are needed here.") Additionally, the national office must contend with the well-recognized problem of detailees looking out for their home agency (or their future careers back at the home agency).

It was an easy matter for the leading CI organizations to withhold authorization for detailees. The military services and DOD's Counterintelligence Field Activity were for the most part supportive of the stand-up of the NCIX, which showed in the quality and consistency of DOD personnel detailed to the office. CIA was forthcoming in providing support personnel, but largely unwilling to assign seasoned CI officers to the staff (which were and remain in short supply within CIA ranks). And despite repeated personal entreaties, the FBI, which consumes the lion's share of U.S. CI dollars and billets, withdrew most of its personnel from the NCIX office, and throughout my tenure did not have a single senior special agent detailed to the staff.[89]

Without the highest quality people, how can a national center do the hard job of leadership and strategic guidance?

Congress sought to address this problem by giving the NCIX direct hire authority. Exercising that authority, however, proved extremely

89 The FBI's assistant director for counterintelligence was a seasoned CI professional who had come up through the ranks, having spent most of his career in the FBI working counterintelligence. He had also been the director's pick to serve as the first NCIX under PDD-75—an assignment that was cut short by the 9/11 attack, when he was recalled to headquarters. Whether his brief tenure as NCIX soured him to the mission, or whether he saw the NCIX as a rival to the FBI's CI authorities, was not clear to me; but his personal predispositions played a prominent role in truncating the FBI's support for the NCIX office.

difficult. First, we needed to establish a new career service to hire people into (one of the many costs distinguishing government from private enterprise), which took nearly a year to work through the CIA personnel system. But a career service implies a career: what kind of upward mobility can a career government servant expect to find in a mini-organization like the office of the NCIX? A total billet structure of 80 to 100 (including detailees) doesn't give much latitude for career progression. Moreover, the head of such an elite office must be extremely careful in making hiring decisions. All sales are final: there is no return to sender option when it comes to direct hire employees, and given the strictures of the career service, firing someone for other than clear cause is very, very difficult. Once an organization has an established reputation for the quality and value of its work, I believe it is possible to recruit and retain a talented core staff—but that happens over time, not overnight.[90]

Accordingly, we turned repeatedly to the well of contract support for talented and experienced personnel. I am particularly indebted to a critical number of retired government personnel who brought special knowledge, expertise, and reputations that were of enormous help to me personally and to the effectiveness of the new NCIX office.

Of course, it is not enough to create and staff a national-level office to head up the CI enterprise. The many parts that make up U.S. counterintelligence must be thoroughly engaged to achieve common ends. And that has proved a much higher hurdle.

One might think that the new office of the NCIX would be welcomed as a powerful advocate of counterintelligence by the leadership of the many CI organizations including in particular the operational entities of the FBI, CIA, and the military services.

90 No sooner had we worked out the modalities of hiring employees directly than the Congress created the DNI organization and all NCIX positions were absorbed into the office of the DNI. I thought this was excellent news. Now people interested in working for the NCIX would also be a part of the much larger DNI organization, with the career mobility that implied. It was also terrible news, because now the little NCIX office would be competing with the big office of the DNI for the limited detailee talent pool—which continues to be a source of tension between the DNI and the many intelligence organizations throughout the government.

While I believe that most of the rank and file held that view, the establishment of the office of the National Counterintelligence Executive was not met with unqualified enthusiasm from all of the CI community leadership. ("Oh good, just what we need: a national office looking over our shoulder and second-guessing our decisions.") Their skepticism may be understandable, since the goal of bringing coherence inherently implies some loss of independence, which is not easy to accept on faith.

Instead, much of the CI leadership adopted a wait-and-see attitude, combined with some forays to test and constrain the reach and authority of the new national office. Not unique to counterintelligence, the bureaucratic bias is inherently conservative, resistant to change (especially when it imposes greater accountability) and favoring the status quo.

And in counterintelligence, the status quo has a long history.

Guiding Principles and Doctrine of the CI Profession

If you are a counterintelligence professional of the U.S. government, what do you do? What are your essential skills? How are you trained? How is your performance evaluated? What is your work product? What defines the CI profession and its mission? There are as many answers to these basic questions as there are adversary intelligence services keeping us busy.

There is no common understanding of what constitutes a CI professional because there is no common undertaking that constitutes the CI profession, and (until recently) no cross-cutting national mission that defines common ends. Instead, each of the operational elements approaches counterintelligence on its own terms and with its own distinctive stamp. Like the butcher, the baker, and the candlestick maker who set up shop on the same street, the CI organizations may be part of the same "community," but their work both individually and corporately is very different. Crime fighter, case officer, or warrior—their approaches to counterintelligence are as varied and independent as their underlying professions.

Find the spies and arrest them. The Federal Bureau of Investigation is far and away America's leading CI agency. Its

preeminent role is the collective result of authorities and responsibilities acquired incrementally over its 100-year history, most in response to national security exigencies.[91] The nation has turned to the investigative resources of the FBI to deal with saboteurs, to find and prosecute spies, and to collect intelligence both domestically and abroad. In the wake of 9/11, the FBI again has been asked to assume expanding responsibilities, leading to the establishment of a new National Security Branch to carry out its counterterrorism and CI work.

In all it does, the FBI remains first and foremost a law enforcement agency, deriving much of its distinctive CI expertise from the techniques and training required for criminal investigations. Ask any FBI agent working counterintelligence, "Are you principally an intelligence officer or a law enforcement officer?" and you will get the same answer every time. The identity that properly comes with carrying a badge and a gun also orders the FBI's core orientation and product line, taking and working each case in turn. Where successful, these cases may result in prosecutions, demarches, or the expulsion of diplomatic personnel for activities inconsistent with their status. But with rare exception, their disposition is decided on the merits of the instant case and not as part of a larger effort to counter the foreign intelligence service as a strategic target.[92]

While the FBI is skilled at enforcing counterespionage and related laws, it has not been organized, trained, or equipped to collect or analyze intelligence on the extensive foreign intelligence presence in the United States beyond those personnel here under official or journalistic cover, or to develop or execute offensive operations to mislead, deny, or otherwise exploit foreign intelligence activities

91 Ray Batvinis, *The Origins of FBI Counterintelligence* (Kansas University Press, 2007)

92 By way of contemporary example, the government's espionage case against suspected Chinese agent Katrina Leung resulted in a 2005 plea bargain with no jail time and a $10,000 fine, in return for which the accused agreed to 10 debriefing sessions about her interactions with the Chinese. The U.S. attorney in Los Angeles entered into the agreement because it served the government's prosecutorial interest in concluding a case that was not going well in the courtroom; but it effectively forestalled CI efforts to engage Leung's future cooperation to learn what national security information she had compromised during her 20 years of passing information to Beijing, or to uncover other Chinese operations against the U.S. government.

against the United States. The FBI may run operations into hostile intelligence services for the purpose of finding spies in the U.S. government (including historically some highly successful ones),[93] but it does not take as its mission running or coordinating operations for the larger purpose of defeating the global operations of an adversary intelligence service.

Make sure our spies succeed. Against the backdrop of the Cold War and the activities of the KGB, counterintelligence at CIA developed largely as a component designed to protect its clandestine operations from compromise.[94] In 1974, a complicated twenty-year history of conceptual, bureaucratic, personal, and ideological struggles within the Directorate of Operations culminated in a purge of the CI staff following public revelations of CIA improprieties. These events led directly to the two-year long session of congressional inquiries by the Church and Pike Committees and an extended public spectacle of further revelations of wrongdoing. In the ensuing years, CIA effectively withdrew from even its narrow CI mission, and has had a long road to recover.[95] The revelation of Aldrich Ames' devastating

93 A stellar example of the FBI's past successes is Operation Solo. Morris Childs was deputy head of the Communist Party of the USA and trusted confidant of his former instructors Yuri Andropov (later head of the KGB and the Soviet Union) and Mikhail Suslov (later the Politburo's chief ideologist). He was also working for the FBI, a penetration effort that continued for 23 years. See John Barron, *Operation Solo: The FBI's Man in the Kremlin* (Washington DC: Regnery Publishing) 1996.

94 "Although the Soviets had recruited more than 200 Americans as spies in the 1930s, 1940s, and 1950s, the United States had done essentially nothing in return." The first significant CIA penetration of Soviet intelligence occurred in 1953 when Pyotor Popov, a lieutenant colonel in the Soviet military intelligence, volunteered his services. He was arrested and executed by the KGB five years later. James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (Virginia: Potomac Books, 2006) 231.

95 To make matters worse, CI and counterespionage (CE) capabilities at CIA declined even more under DCI Stansfield Turner (1977-1981), whose book, *Secrecy and Democracy: the CIA in Transition* (Boston: Houghton Mifflin, 1985), reveals his strong biases against CE. As reviewed by Robin Winks, Turner "asserts a variety of positions—such as his contention that the sudden reduction of the espionage staff by 820 positions did no damage to national security—without offering evidence or argument to support his view. He appears to believe that a CE capacity is not needed because SIGINT has

betrayals in the service of the Russians sparked a painful reappraisal of CIA's counterespionage capabilities and the establishment of a dedicated senior CI office on the 7th floor (i.e., the director's suite). That position was abolished in the latest reorganization, which assigned CI responsibilities to a staff element within the new National Clandestine Service, whose duties are yet to be fully defined.

While any CIA clandestine officer will tell you that foreign intelligence personnel are already at or near the top of their targeting list, it is one thing to check the box for recruitment opportunities, and quite another to have a top-down strategically orchestrated effort to disrupt and degrade the operations of a foreign intelligence service. Indeed, there is an inherent tension between the work of human intelligence (HUMINT) collectors and that of strategic CI operations. Intelligence collection values, above all, the information; counterintelligence insists on acting on that information, which introduces new risks. For example, if a penetration within a foreign government were used as a CI asset (such as serving as a channel for deception), that CI operation would introduce a new risk of compromising the asset, to the potential detriment of the collection effort.

So far from being a partner with the FBI to build a global perspective on the operations of foreign intelligence services, CIA has interpreted its CI job as confined to protecting its own house and mission. During the Cold War, the Directorate of Operations correctly understood one of its primary tasks, the clandestine penetration of the KGB, to be an important contribution to the overall, but generally undefined, national U.S. CI mission. But CIA was not directed and

---

replaced HUMINT, incidentally removing the many risks of human error that arise from HUMINT; he then redefines disinformation to suit his own needs and concludes that the only CE requirements the United States has are to deal with domestic spying. Since the FBI handles the home front, CE has no role to play….He recommends that the espionage and analytic branches should be merged in order to make CE a team player. This sounds a good idea if one believes that intelligence is still a game, great or otherwise, but it flies in the face of the rudimentary methodology of compartmentalization. The need is less to make CE play for the team than to find a way to see to it that a necessarily somewhat independent operation does not try to steal a base out of a misplaced sense that the coach doesn't know what to do." Robin Winks *Cloak and Gown: Scholars in the Secret War*, 1939–1961 (New York: William Morrow, 1987) 547–548

did not attempt to create a worldwide CI service designed to detect, analyze, and counter all foreign intelligence operations abroad that were directed at the United States and its interests.

Protect against enemy intelligence operations. Counterintelligence at the Defense Department is grounded in the larger force protection mission of the military services. Each of the military services charters and organizes its relatively narrow CI efforts substantially differently, to meet Service requirements. The Army combines its counterintelligence function with those of human and signals intelligence under the assistant chief of staff for intelligence; its CI officers have no criminal jurisdiction. The Air Force and Navy, on the other hand, keep counterintelligence separate from their intelligence functions and combine CI duties with criminal investigation. The Air Force component, the Office of Special Investigations, reports to the Air Force inspector general, while the Navy Criminal Investigative Service is a separate command within the Navy Department.[96] As is common to other functions within the hierarchical organization of the Defense Department, each combatant commander also has a CI staff element, while the Services organize, train, and equip the Service CI components assigned to support the combatant commands.

With each of the military service components looking to its own needs, until recently there was no entity charged with the CI concerns of the many independent Defense agencies, activities, and non-Service personnel, or one that could bring a cross-cutting, strategic perspective commensurate with the size and importance of DOD assets as targets for foreign intelligence collection and manipulation. To redress this deficiency, the Counterintelligence Field Activity was established in 2002 within the Office of the Secretary of Defense to develop and manage all DOD CI programs, and to serve as the central coordination point for CI policy and budget matters within the Department. Unfortunately, the CI Field Activity suffered the bureaucratic equivalent of the perfect storm when it was buffeted from two directions—a scandal involving a Congressman on the take from its lead contractor, and public concerns over DoD's involvement

96 In addition to the Service components, the 650th Military Intelligence Group in support of the North Atlantic Treaty Organization also has authority to conduct offensive CI operations; the secretary of defense may designate others.

in domestic surveillance—resulting in a much weakened, smaller organization struggling to define its role.

The Department of Defense owns or controls most of the secrets worth stealing, but it does not command the suite of resources necessary to counter foreign intelligence operations directed against those secrets. Nor does it have the authority to take on that mission alone. Executive Order 12333 requires that DOD coordinate its CI operations abroad and at home with CIA and FBI respectively, which have lead CI responsibility in those domains; accordingly there is substantial bilateral interaction and deconfliction among the CI components. But deconfliction falls far short of strategic integration—a job not assigned to the Defense Department nor any of its sister CI agencies.

In the absence of a lead department or agency, or central leader, or common service, the larger strategic mission of counterintelligence in support of national security objectives does not have a dedicated national CI profession organized, trained, or equipped to carry it out. Today's CI personnel lack even many of the basic training and education programs needed to help them understand the larger context in which they work, or to acquire the necessary skills individually and jointly to perform the critical national security mission they are being asked to assume.[97] Interagency training falls far

97 I commissioned an interagency study to look at core competencies for the CI profession, which found its way to my desk on my last day on the job. It found a severe gap between contemporary CI performance requirements and our ability to train and develop a professional CI cadre: "Training programs are limited primarily to initial skills training with a general lack of structured continuing education programs… Because CI lacks the training infrastructure to support long-term development of the individual, there is no accepted career path for the counterintelligence workforce…As a result, counterintelligence assignments are generally not seen as career enhancing and many individuals tend to move on to what they see as mainstream assignments in their respective organizations… A compounding factor has been a lack of CI leadership development. Many senior CI positions are filled with individuals who lack significant CI experience and training." Office of the NCIX, *Fundamental Elements of the Counterintelligence Discipline*, Volume 1 "Universal Counterintelligence Core Competencies" (Unclassified Version January, 2006) 4. Overall, the ranks of CI professionals are thinning, which has adversely impacted the management tier of U.S. counterintelligence and further limited the pool of available talent for

short of what is needed to enable integrated operations, and there is almost no interdisciplinary training across CI specializations.[98]

Across the profession, there are vast differences in understanding of what counterintelligence means, and how it is done, and even the basic terminology it employs.[99] In the face of such fundamental disunity, is it possible to tie together the nation's many CI activities in order to defeat foreign intelligence threats to the United States?

The need for a common CI doctrine. Each of CI's operational elements has answered a different call, with historical origins and continuing requirements that have led to specialized functions, techniques, and missions. While bilateral cooperation and coordination are not uncommon (especially in the wake of 9/11), to speak of a CI "community" is to stretch the meaning of the word. But that is not all bad news.

As I see it, the very diversity of U.S. counterintelligence is an essential part of its strength. Each of the distinct operational approaches to counterintelligence has distinctive advantages. Pulling the best from each, carrying those skills and techniques across to sister elements, and integrating and coordinating their efforts can result in a tremendous national asset to counter foreign intelligence threats. But

assignments outside of line agency duties (including in particular national or interagency billets).

98 CI practices employed by intelligence agencies may be very useful for law enforcement agencies now faced with the need to gather intelligence against potential terrorist cells within the United States, but these are skills that must be carefully taught. Consider, for example, the "counterintelligence review," which seeks to determine the reliability of human intelligence assets through a careful and stylized examination of the asset's entire case file, from recruitment through production. See Brian Kelley, "Counterintelligence Applications to Law Enforcement," *Crime & Justice Internationa,l* Vol 23, No 99, (July/August 2007) 30, 33–34. Such CI practices have been developed over decades, the skills cannot be learned on the fly, the generation of necessary mentors is leaving or has left government service, and experienced teachers are in short supply even on the home turf of their (former) home agency much less in the unfamiliar classrooms of law enforcement agencies.

99 In attempting to compile a lexicon of agreed CI terminology, my staff ran into such fundamental disagreement over a number of basic terms that the effort never came to closure. In particular, "offensive counterintelligence" has very different meanings to different parts of the community.

we need to have laid sufficient common ground for the profession as a whole in order to make strategic integration viable.

The key missing ingredient is a common *doctrine* for U.S. counterintelligence, a body of common institutional thought that relates the reach and characteristics of U.S. CI activities to the national security objectives of the United States. As defined by the Defense Department, doctrine consists of the "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives."[100] The purpose of developing a doctrine is not to constrain creativity but to enable its effective employment; hence doctrine "is authoritative but requires judgment in application."[101] Having a common body of concepts or principles is the essence of a professional mission. Yet, for all its rich history, counterintelligence does not have an agreed body of working principles or a settled conceptual approach to guide the application of means to ends.

For example, there is a widespread lack of understanding of the difference between counterintelligence and security. In practice and by executive order, counterintelligence is closely related to, but distinct from, the security disciplines.[102] Sound security measures are unquestionably vital, but they can carry protection only so far. One can pile on so much security that no one can move and still there will be a purposeful adversary looking for ways to get at what it wants. The defining job of counterintelligence is to engage and confront the adversary, yet this imperative too often is neglected

100 Joint Publication 1-02, "DOD Dictionary for Military and Associated Terms"

101 Ibid.

102 The practical objectives of CI and security are not always in concert – which Christopher Felix (true name James McCargar) called "one of the classic conflicts of secret operations." Counterintelligence "operations are offensive operations which depend for their existence as well as success on constant, if controlled, contact with the enemy. Security, on the other hand, is a defensive operation which seeks to destroy the enemy's operations and to cut off all contact with him as dangerous." Felix, *op cit* at 126. But the interdependency between CI and the security disciplines has led to some long-playing theoretical discussions about which—if either—may be said to encompass the other; in practice, at a minimum, the two must be closely linked.

especially as we think about the place of counterintelligence in national security planning.

Does it matter that counterintelligence does not have a common doctrine? It may sound quaint today, but the formative years of the U.S. Air Force included a vigorous debate over this missing element. Fifty years ago, Air Force leaders, arguing over the meaning of air superiority, observed that the Air Force as a service lacked a clear set of ideas against which it was operating. As one scholar of the era observed,

Without such principles and concepts being clearly expressed, at least in the minds of the users, it is not at all possible to attain coordination and efficiency, and it is not reasonable to expect, as is desirable, that all workers to the common end will have in mind the same possibilities and objectives. [103]

> The extraordinary accomplishments of the modern Air Force are owed in no small part to its essential rigorous intellectual grounding in agreed doctrine.

Similarly, CI professionals need to have an intellectual framework to guide their work as part of the larger national enterprise. To succeed as a tool of national strategy, counterintelligence needs to be more than a come-as-you-are party. The widespread lack of understanding of the strategic CI mission, not to mention the lack of a consensus on how to proceed, will persist so long as there is no professional doctrine to enable its execution.

Of course, even if the profession were to develop a body of thinking or doctrine to enable coordination across the many tactical department and agency activities, along with the needed training and education programs, we still would need to set out the strategic goals and objectives for the national CI mission.

And that is where *The National Counterintelligence Strategy* enters the picture.

---

103 Robert Frank Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force 1907-1960*, Volume I (Maxwell AFB, Alabama: Air University Press, 1989) 1

Mechanisms for Decision Making

The number one responsibility of the NCIX is to develop each year, for the president's approval, a national strategy to guide U.S. counterintelligence, and then to see to it that the strategy is in fact executed. These are vastly different duties, but the principal interagency mechanism intended to oversee them is the same: the National Counterintelligence Policy Board. [104] During my tenure, the Policy Board, which is chaired by the NCIX, proved a useful forum to review and coordinate the first national counterintelligence strategy, but of little value in effecting its execution.

National strategies are in vogue. The National Security Strategy of the United States was first mandated in law as part of the 1986 Goldwater-Nichols Act.[105] Initially envisioned as an annual report but currently issued every four years, the National Security Strategy is intended to inform subordinate strategies including those for combating terrorism, WMD, and illegal drugs, and those for securing cyberspace and critical infrastructure. Following 9/11, there is also a Homeland Security Strategy and related strategies (maritime security, border security, aviation security, etc). The secretary of defense issues a national military strategy as required by law,[106] and in 2005 the DNI issued a national intelligence strategy on his own initiative. But that is not all.

There are national strategies to meet specific objectives (e.g., the "National Strategy for Victory in Iraq"), and to engage international support (e.g., "National Strategy to Internationalize Efforts against Kleptocracy"). There are national strategies to reduce congestion

104 Recognizing the overlap between the board's statutory duties (as set forth in the Counterintelligence Enhancement Act) and the NSC Policy Coordinating Committee for Intelligence and Counterintelligence (established by the president in NSPD-1), the NSC staff and I quickly agreed that whenever the board met for purposes of advising the president it would sit also as the PCC for Intelligence and Counterintelligence, and that the NSC senior director for Intelligence would co-chair the meeting along with the NCIX—a practical and beneficial arrangement for all parties that has stood the test of time.

105 Section 108 of the National Security Act of 1947, as amended; 50 U.S.C. 404a.

106 10 USC 113(j)

on America's highways, to cut poverty in half, and to reduce gun violence. There is a national strategy for agriculture and another for federal archeology, a national strategy to promote financial literacy and another to restore coastal habitats. There are a number of national healthcare strategies including strategies to prevent suicide, teen pregnancy, and pandemic influenza, and strategies to advance immunization quality and oral health. The list goes on.

These national strategies are as varied in quality and impact as they are in subject matter. Each may have its place and constituency, but I wonder if the importance assigned to national strategy has not faded by reason of the proliferation of these documents. Much of their content is declaratory policy or public relations masquerading as strategy—important publications in their own right but different from the integrating coherence strategy is intended to supply. Certainly some bureaucracies have become accustomed to treating these strategies less as controlling guidance for developing policies, plans, and programs than as cover for continuing business as usual.

With all good intentions, Congress contributes to devaluing the coin of national strategy when it requires that a new strategy be issued each year. Whatever else a national strategy may be, it should import a sense of vision, endurance, and longer range goals against which to array shorter term plans and programs. If the bureaucracy comes to expect a new strategy every year, how can any given strategy be effective? By the time it is issued, the federal government is already entering into the next year's budget cycle, including the underlying plans and programs that drive the allocation of resources. National strategies that become obsolete after one year simply cannot be taken seriously.

Against this backdrop, I had the pen for the first draft of the first ever National Counterintelligence Strategy of the United States. The document drew on the thoughtful contributions of long-time practitioners and scholars assembled early in my tenure for a three-day conference held at the McCormick-Tribune Foundation's Cantigny Estate to consider the state of U.S. counterintelligence and the need for strategic direction. I also had invaluable help from some of the nation's most outstanding CI experts who served on my staff.

To begin, we turned to the National Security Strategy of the United States, which President Bush had approved in 2002. That document

is organized around the major challenges confronting America's security—defeating global terrorism, countering weapons of mass destruction, ensuring the security of the homeland, transforming defense capabilities, fostering cooperation with other global powers, promoting global economic growth—each of which has an embedded counterintelligence imperative. Specifically, terrorists and tyrants, foreign adversaries and economic competitors, engage in a range of intelligence activities directed against the United States in order to advance their interests and defeat U.S. objectives. It is the job of U.S. counterintelligence, subject to national policy direction and in concert with other instruments of national power, to see that they do not succeed.

National CI Policy Board Membership

NCIX, Chairman

Department of Justice

Federal Bureau of Investigation

Department of Defense

Joint Chiefs of Staff

Department of State

Department of Energy

Central Intelligence Agency

Department of Homeland Security*

NSC Senior Director for Intelligence, *ex officio*

**added by President Bush*

It may seem strange that national strategy governing an undertaking of such extreme sensitivity as counterintelligence could be written at the unclassified level and still be meaningful. Yet the simple fact is that the most important attribute of the new strategy was its very existence: the declaration of a unified national purpose and the assignment of strategic roles and missions to the nation's counterintelligence enterprise. In our democracy, these matters are properly the subject of public information and debate. Accordingly, I argued (and the Policy Board agreed) that the first iteration of the National Counterintelligence Strategy should be unclassified, so that it could receive the widest possible dissemination and attention not only within the counterintelligence community but also among the nation's national security leadership and the public at large.[107]

107 In furtherance of that purpose, the 2005 *National Counterintelligence Strategy of the*

I distributed the draft to the members of the National Counterintelligence Policy Board, who are charged by law with advising the president on counterintelligence policy and advising the NCIX on the implementation of the strategy. In keeping with review practices for national security strategies that bear the president's signature, I asked that board members treat the document as "close hold" in order to preserve the president's options, and that they give the draft the personal and careful attention it merited as the first national strategy to guide our common enterprise. This inaugural document would become the foundational "vision" statement of the mission of counterintelligence in service to national security, and we needed to be very sure that we got it right.

The interagency coordination process resulted in some textual changes, including a number of substantive additions that strengthened the document. I also received unusual written clearance from the FBI, which foreshadowed rough times ahead. The FBI representative declined to comment on the draft; instead he sent a short note, thanking me for the opportunity to review the draft and enclosing a copy of the FBI's two-year-old internal CI strategy—with no other comment. In other words, the FBI representative was saying, "You can do what you want. Here is our strategy. Live with it." The FBI's counterintelligence division published another so-called "national strategy for counterintelligence" two months after the President's strategy was issued. The two documents bore little resemblance to one another; indeed, the FBI's strategy never even acknowledged the existence of the national strategy that the president had approved.[108] Individual department and agency strategies can and should be valuable

United States is included here as Appendix B2.

108 As of this writing, the FBI's webpage and public comments continue to feature its own "national" counterintelligence strategy with no reference to the strategy approved by the president. Contrast congressional testimony by the FBI's Assistant Director (Counterintelligence Division): "Our National Strategy will be totally integrated with the Office of the National Counterintelligence Executive (NCIX), or CI-21, to ensure that our efforts are focused on policy driven priorities…". David Szady, "Changes the FBI is Making to the Counterintelligence Program," Hearings before the Committee on the Judiciary, United States Senate, April 9, 2002.

planning documents. But if they are developed and promulgated independent of national-level guidance, what is the point?

With the concurrence of all members of the Policy Board, the draft National Counterintelligence Strategy was submitted to the staff of the National Security Council in April of 2004, for internal review within the Executive Office of the President.

And there it sat for almost a year, sidelined by NSC staff ostensibly worried about getting out of step with related developments including the looming debate over creating a new national intelligence director. Finally, a somewhat abbreviated (but substantively unchanged) draft was forwarded to the President for his review and approval, and transmitted to the Congress March 31, 2005.

The National Counterintelligence Strategy was released to the public at a national conference on counterintelligence, held at the Bush School for Intelligence at Texas A&M. (Indeed, the firm date of this long-planned conference was the precipitating factor that moved the draft strategy out of the staff's in-box and onto the president's desk.) President George H.W. Bush gave the opening address, community participation was robust, press coverage was excellent, and the National Counterintelligence Strategy had the most promising public roll-out possible.[109]

But we had lost a year of precious time, before U.S. counterintelligence could turn to the even greater challenge of implementing the president's strategic guidance.

Executing and implementing national direction

In my view, there is little possibility of implementing unified national direction without a sense of common purpose. Among its other attributes, I envisioned the office of the NCIX supplying the common ground needed to build community and to identify common purpose. And what better way to start than with a party.

109 *Washington Post*, "U.S. Adopts Preemptive Counterintelligence Strategy" March 6, 2005, A07; *Washington Times,* "U.S. Targets Foreign Spy Services," March 6, 2005, A1

The ribbon-cutting on the new NCIX office brought people together from across the CI community, many of whom were meeting one another for the first time. The outer lobby was carefully designed to invite lingering, its four walls covered with museum-quality displays chosen to educate visitors about the four dimensions of our craft: the origins of CI in America, the tools of the trade, the global reach of adversary services, and the "wall of shame" – a portrait gallery and case summaries of traitors and convicted spies. *Washingtonian Magazine* did a feature story (something along the lines of "Washington lobbies that tourists will never see"), the Director of Central Intelligence gave a welcoming speech, and there was a sense that building a genuine CI community was an achievable goal.

The implementation of the first *National Counterintelligence Strategy* would put that community to the test.

Executing and implementing national direction for counterintelligence is a four-fold decision-making process, each involving different parts of the national security apparatus:

- First, national security policy guidance, from which national CI strategy is derived.

- Second, national strategy to direct the CI enterprise, from which implementation plans are derived.
- Third, annual planning, programming and budgeting, to conform government-wide resource allocation to national priorities.
- Finally, strategic operational planning, through which strategic CI objectives are achieved.

In each of these areas, we made some progress; but the lingering question is whether these modest beginnings will take hold.

1) Policy guidance. In order for counterintelligence to serve as an instrument of national security strategy, it must be integrated into the national security policy process. The *National Counterintelligence Strategy* expressly calls for CI to have a seat at the policy table, where owing to its disaggregated history CI has not appeared before. But once it is understood that the strategic purpose of counterintelligence is to identify, assess, and defeat foreign intelligence threats to U.S. national security objectives, the need to tie CI functions into National Security Council deliberations and the larger policy context becomes compelling. In national security policy planning and execution, we have learned that U.S. intelligence operations and especially covert action must be integrated into the broader strategic picture to judge properly the cost/benefit operational risk and correctly gauge the allocation of resources. The same is true for CI operations, which must be considered in the context of the broader national security purpose if they are to have strategic effect.

The allocation of CI effort (i.e., which foreign intelligence services should be the highest priority targets of CI activities to assess and neutralize their operations?) needs to be driven by national security considerations. Left to its own devices, with no policy guidance, the U.S. intelligence community will rank order foreign intelligence threats on the basis of their capability to threaten U.S. intelligence operations. The impact of foreign intelligence operations on U.S. collection and intelligence production is a key consideration, to be sure, but it is far from the only measure of concern. To bring strategic guidance to the U.S. CI effort, the prioritization of foreign intelligence threats must align national security policy concerns and CI resource allocations,

rather than simply itemize what is known about foreign intelligence capabilities.

NSC leadership welcomed CI analytic input, and in those instances where we had sufficient advance notice of key policy deliberations we were able to contribute useful insights and ideas. But the relationship between the CI world and senior national security policy makers was largely personality dependent and tasking was *ad hoc*, rather than a routine way of doing business. The DNI regularly sends a representative to NSC-led interagency meetings to provide intelligence support, but CI analytic input is included only sporadically and CI operational options rarely if ever are factored into the national policy debate. And we still lack an effective means by which policy leaders can guide CI priorities.

This gap between national security policy attention and CI effort reflects what may be the single greatest weakness in the national CI mission today. By and large, the national security policy community seems unaware or unconvinced of the dangers to U.S. national security posed by the intelligence activities of foreign powers. This is yet another troubling legacy of our Nation's historical non-strategic approach to counterintelligence, which remains largely unaddressed.

For all of the good work of its contributors, the "CI-21" study of the late 1990s did not make a convincing intellectual case that identifying and neutralizing (or exploiting) foreign intelligence activities must be a part of U.S. national security strategy and policy. Nor did Congress, in enacting the Counterintelligence Enhancement Act of 2002, assign the strategic CI mission a purposeful role in national security planning.

It is up to the president and his policy leadership to judge the importance to U.S. national security of countering foreign intelligence operations and to issue policy guidance based on those judgments. But first they need to be presented with the essential insights into foreign intelligence plans, intentions, and capabilities to be able to assess their impact on U.S. national security, which presents somewhat of a chicken-and-egg problem. The intelligence community will not turn its resources to collect and analyze foreign intelligence activities as an input to inform policy makers unless so tasked; but with little to no insights into foreign intelligence activities, there is nothing to alert the policy maker to the threats they present.

The National Counterintelligence Strategy made an important beginning in breaking this impasse by explicitly linking policy guidance to CI effort for the first time. It also directs the integration of CI information and operational options into national security decision making in order to educate and inform both communities about threat and opportunity. The modalities for coupling national security policy direction to strategic CI output are not difficult to devise, but it remains for them to be institutionalized into daily business.

2) Implementation plans. The 2005 *National Counterintelligence Strategy* set forth the standing mission of U.S. counterintelligence in support of national security. Its seven pillars defined major goals for the counterintelligence enterprise to 1) counter terrorist operations, 2) seize strategic advantage, 3) protect critical defense technology, 4) defeat foreign denial and deception, 5) level the economic playing field, 6) inform national security decision making, and 7) build a national CI system. In particular, its emphasis on proactive strategic operations set a new and high bar for U.S. counterintelligence.[110] But the document is not a strategy in the classic sense of setting forth the means to accomplish defined ends; rather it established broad (and unclassified) objectives, each of which require detailed strategic planning to achieve.

Above all, the *National Counterintelligence Strategy* called for a reorientation of the U.S. CI enterprise to go on the offense. This was far from a new idea; indeed, it is the first "commandment of counterintelligence," as captured in an excellent article by a former head of CIA's Counterintelligence Center:

CI that is passive and defensive will fail. We cannot hunker down in a defensive mode and wait for things to happen. I believe we are spending far too much money on fences, safes, alarms, and other purely defensive measures to protect our secrets. That is not how we have been hurt in recent years. Spies have hurt us. Our CI mindset should be relentlessly offensive. We need to go after our CI adversaries.[111]

110 For more on this point, see my article, "What Is Strategic Counterintelligence, and What Should We Do About It?" *Studies in Intelligence* 51:2 (Washington, DC: Center for the Study of Intelligence) June 2007, 1–14.

111 James Olson, "The Ten Commandments of Counterintelligence," *Studies in*

The first National Counterintelligence Strategy took this time-honored commandment into the realm of national strategy—and in so doing, made a sharp departure from the past.

Historically, instead of looking at the strategic implications of foreign intelligence operations, the U.S. government for the most has part adopted a case-by-case approach to dealing with the threat they represent. By concentrating our CI resources overwhelmingly within the United States, rather than engaging the foreign intelligence service abroad, we have ceded the advantage to the adversary. Foreign powers have seized the initiative, and moved their operations to U.S. soil, where our institutions are not constituted to work against the growing foreign intelligence networks embedded within American society. Consider how it is that spies within the very heart of U.S. intelligence and the national security community have been able to operate undetected for such unacceptably long periods of time (for example, Ames, nine years; Robert Hanssen, twenty-one years; Ana Belen Montes, seventeen years; the unindicted Katrina Leung, twenty years) to the profound detriment of U.S. national security. Interagency damage assessment teams are quick to key on exploitable security vulnerabilities and to recommend new security measures (e.g., more uniform polygraph practices, more rigorous background checks, more comprehensive inspection regimes, more sophisticated information system audit trails). But smarter security alone will never be enough so long as the foreign intelligence adversary retains the strategic advantage, which we have ceded by default.

The National Counterintelligence Strategy directs that the considerable resources of the members of the U.S. intelligence community that have global reach be prioritized and coordinated in order to degrade the foreign intelligence service and its ability to work against the United States, starting with working the target abroad. The tradecraft and operations of counterintelligence are not new. What is new is the policy imperative to integrate CI insights into national security planning, to engage CI collection and operations as a tool to

Intelligence, (Washington, DC: Center for the Study of Intelligence) Winter-Spring 2001.

advance national security objectives, and, at the strategic level, to go on the offense.

If a national strategy is to progress from well-formulated ideas to well-executed results, it must have effective implementation plans. While it is properly left to national leadership to define national objectives, identifying the means of achieving those objectives requires collaboration among those who command the resources, people, and programs involved in their execution. This is the point at which component leadership is most important. Broad goals are fairly easy for department and agency representatives to endorse; but signing up to specific implementation plans means subjecting performance to external measures of effectiveness, which bureaucratically is far more onerous.

The members of the National Counterintelligence Policy Board evinced little interest in ensuring that the *National Counterintelligence Strategy*, with its challenging proactive orientation, was in fact implemented. Despite the Policy Board's statutory mandate to advise the NCIX on implementing national strategy, I never received a single call, paper, inquiry, or suggestion on implementing any of the strategy's broad goals or specific objectives. Members attended Policy Board meetings to receive and exchange information, but we were not overly burdened by lively discussion. There were several reasons for this.

Counterintelligence is inherently a close-hold business, which serves as a natural constraint on interagency discussion. This reticence was magnified by the fact that the department and agency representatives to the Policy Board varied widely in the scope of their responsibilities and in their personal knowledge of counterintelligence. This disparity put a damper on the effectiveness of the Policy Board as a forum for discourse. The four board members with major and direct CI operational responsibilities saw little to be gained from sharing their observations with a 10-member interagency group, while other members with broader (and largely non-CI) duties were only tangentially conversant with CI concerns.

More generally, senior-level interagency policy bodies have proven quite successful as a modality for finding consensus among differing perspectives, but in my experience they are far less fruitful as deliberative bodies to explore creative approaches to national-level

concerns. Members readily understand their role as advocates of their own department or agency brief, but are usually less comfortable reaching beyond their own portfolio to offer objective thinking or advice on broader national needs. I believe it is possible, given the right mixture of personalities and challenges, for an interagency committee to grow into a productive forum for creative thought, but that quality is more the exception than the rule.

In short, the Policy Board as constituted during the period of my chairmanship never measured up to the constructive advisory body the Congress envisioned to help execute national CI strategy. Some of my choices as chairman may be partly to blame for this failure. I have an aversion to calling meetings just for the sake of meeting: if there are no actions to be taken or decisions to be made I would rather not impose on everyone's time. My forbearance in convening meetings may have been appreciated by busy department and agency representatives but it also limited opportunities for building useful group dynamics. Nor did I deem it practical to assign individual Policy Board members the responsibility for devising implementation plans, which inherently require interagency collaboration and input across the CI community.

With these considerations in mind, implementation planning for the new strategy would have to be accomplished through other means.

In order to carry out the broad mandate of the office of the NCIX to integrate and coordinate U.S. counterintelligence, it was clear from the outset that we would need a basic interagency infrastructure to enable communication and interagency coordination.[112] We established the CI Steering Group, chaired by the Deputy NCIX, to consider major policy issues, along with subordinate working groups for analysis, collection, operations support, programming and budget, and training and education. The Steering Group was a "big

112 I also believed it was vital to have a means of sharing information and communicating guidance across the CI community. To that end, I established a regime of National Counterintelligence Advisories, Directives, and Requests for Information, starting with NCID-1 which set forth their purpose and functions. Those few early communiqués were superseded when the office of the NCIX was folded under the office of the DNI.

tent," inviting participation from any government organization with a counterintelligence mission, while its subordinate working groups were more selective in membership and focus.

To jump start interagency implementation planning, my staff drew up a logic tree, listing the seven major goals or pillars of the *National Counterintelligence Strategy* from which candidate strategic objectives were derived. Under the auspices of the CI Steering Group, representatives from across the CI community volunteered to lead each subject area, to review and validate the subordinate strategic objectives, and (with the assistance of the functional working groups) to develop top-level implementation plans, assigning roles and missions to the executing agencies. The implementation plans in turn were presented to the CI Steering Group for review and approval; and any matters in disagreement that the Steering Group could not resolve were to be forwarded to the Policy Board for resolution.

This process, while laborious, was essential to engaging community buy-in—not only to the broad goals of the strategy, but also to a new way of doing business that required deliberation and consideration across the CI enterprise. We placed a premium on the broadest possible community participation, and in that we were successful. But our very success is a classic good news/bad news story, as anyone who has ever been involved in interagency working groups or clearance processes can attest. For every creative new participant contributing to the effort, one could also find a new critic interposing objections on behalf of his or her agency, including some who wanted to revisit the language of the strategy itself—even though it had already been approved by the president.

Strategic CI Assessments

Strategic assessments of foreign intelligence capabilities can also help inform policy deliberations and frame options for actions. For example:

- If the United States is confronted with the prospect of war with Iran, what role will Iranian intelligence services play in conducting operations against the United States and what options do we have to neutralize those operations?
- If North Korea attempts to sell and deliver a nuclear device or nuclear materials, what contribution can our counterintelligence forces make in the efforts to detect and intercept such activities? *(continued)*

Yet slowly but surely the necessity of exploring how to implement the new Strategy interjected a new dynamic into the interagency, pointing in the direction of more purposeful national planning and integration of effort. This phenomenon is part of the enduring wisdom of "build it and they will come." But nobody promised it would be quick.

- What hostile intelligence activities are directed against the United States that might be designed to neutralize our capacity to exercise effective space control?
- To what extent are the intelligence elements of the governments of South Korea and Taiwan susceptible to deception by hostile intelligence forces and do we have sufficient capability to discern those operations and guard against efforts to misdirect us?
- What is the role of Cuban intelligence personnel in Venezuela, and what influence does Havana exercise over Chavez's government?
- What efforts are underway by hostile intelligence forces to undermine the effectiveness of our ballistic missile defense system? How effective are our security preparations in protecting against these actions?

As fate would have it, just as we were challenging the CI community in designing these implementation plans for the *National Counterintelligence Strategy*, the DNI came out with a new national intelligence strategy, which similarly required the development of strategic objectives and implementation plans to meet them. While not inconsistent with the *National Counterintelligence Strategy*, the new policy goals of the Intelligence Strategy commanded priority time and attention from the intelligence community, which had the effect of relegating the strategic reorientation of the counterintelligence enterprise to a second-order concern.[113] My sense was that the

113 Counterintelligence is mentioned in three places in the Intelligence Strategy, quoted here in their entirety.

First, counterintelligence is included among the Key Goals summarized in the Introduction: "Deploy effective counterintelligence measures that enhance and protect our activities to ensure the integrity of the intelligence system, our technology, our armed forces, and our government's decision processes." Second, the NCIX is given specific tasking for priority analysis: "[T]he National Counterintelligence Executive will devise plans to enhance analysis of terror networks and foreign intelligence establishments and activities. The latter

intelligence community was a little over-loaded by these time-consuming national-level strategic planning requirements, which if not done well become an end in themselves rather than an effective tool to guide operations.

By the time I left office, the outlines of some of the strategic CI implementation plans were beginning to emerge; but it had taken far too long to get the process up and running. I was hopeful, however, that the process would function more smoothly in the future, once it was established that interagency implementation planning would be the means by which key strategic CI milestones were established and progress evaluated. But that good outcome requires some continuity in national strategic guidance so that planners can have something enduring to build on, and some discipline over the allocation of resources, so that departments and agencies are held accountable for meeting implementation milestones. These requirements have yet to be met.

CI Steering Group Members

Army Assistant Chief Staff (Intelligence), Air Force OSI

Central Intelligence Agency

Coast Guard

Counterintelligence Field Activity (DOD)

Defense Intelligence Agency

Energy Department

Defense Security Service

Defense Threat Reduction Agency

Federal Bureau of Investigation

Homeland Security Department

Joint Staff J2

Justice Department

Missile Defense Agency

(continued)

plan will include a means to integrate counterintelligence with other sources to capitalize on opportunities for strategic offensive activities," echoing the proactive orientation of the *National Counterintelligence Strategy*. Finally, in the section on improving security, the Intelligence Strategy sets forth a requirement to "ensure the various Intelligence Community elements conducting counterintelligence activities act as a cohesive whole to undertake aggressive, unified counterintelligence operations… The National Counterintelligence Executive, in the plan for implementing the National Counterintelligence Strategy, will describe how the Community will undertake aggressive counterintelligence operations with greater unity of effort." Given its lack of directive authority, the limited charge to the NCIX to "describe" how the Community might achieve a greater unity of effort is sadly about right.

3) Planning, programming, and budgeting. Strategy establishes broad national goals, implementation plans establish milestones to carry out strategic objectives, and then the individual agencies are responsible for supplying the means needed to achieve them. In the federal government, the annual budget cycle is the formal analytic structure through which planning, programming, and budgeting is disciplined, to match resource allocation to national priorities, and to evaluate effectiveness. It is also the point at which things can fall apart.

National Geospatial Intelligence Agency National Nuclear Security Agency

National Reconnaissance Office

National Security Agency

Naval Criminal Investigative Service

State Dept Office of Diplomatic Security

State Dept Office of Intelligence & Research

Under Secretary of Defense (Intelligence)

NSC Senior Director for Intelligence, *ex officio*

It is one thing to define national strategy and its derivative objectives; it is quite another to align policy, plans, programs, and resources aggregating across multiple disconnected agencies to meet those objectives. The task of baselining current capability (itself a formidable job) and then working forward, demands an ongoing, iterative process of cross-cutting evaluation and feedback and course correction across the several departments and agencies with CI accounts. As our experience would show, this is a notoriously difficult process in government and arguably impossible without central budget control—an authority not granted the NCIX.

The establishment of a new overarching national office, like many other legislative initiatives, is almost always the product of compromise. Powerful and influential cabinet secretaries with weighty missions to perform naturally have champions on the Hill looking out for their interests (and the prerogatives of their own committees). As a result, national offices may be given new authorities, but within careful limits. Thus it is that an office such as the NCIX can be assigned the statutory mission to lead, integrate, and coordinate all U.S. counterintelligence, but be confined to an advisory role only when it comes to budgets, people, and programs.

While by law the NCIX office is given responsibility to provide strategic direction to U.S. counterintelligence, it does not have the power to direct budget allocations. It is given the responsibility to evaluate department and agency performance, but it is not given the power to direct programmatic changes. The DNI could ameliorate this deficiency by delegating his budgetary and program direction authorities over counterintelligence to the NCIX, but he has chosen instead to vest those in his line deputies rather than in the NCIX. As a result, the modest authority granted the NCIX over the CI community was further diluted when it became clear that the Deputy DNI for budget and administration would exercise the DNI's authority over the counterintelligence budgets, rather than the NCIX. To be sure, the deputy DNI solicited NCIX input, but that input was clearly received as advice (which the deputy DNI rejected on more than one occasion) rather than as authoritative guidance.

It may go without saying, but without the power of the purse to direct resource realignment to meet national needs, there is little hope for national direction to trump individual department and agency priorities. If there is no effective means of holding agencies accountable for meeting national objectives that go beyond the individual responsibilities driving their budgets, there is no possibility of managing to effect. Our experience with national CI direction was no exception.

But that was not the biggest problem.

Each of the CI components was asked to map their programs and resource allocations against the new national strategic CI objectives. And each of the several CI components brought forward their planning documents, and presented their budgets for review, as requested.

Miraculously, all existing department and agency CI plans, programs, and budgets matched perfectly to the new national strategic priorities. No real changes were needed. No new starts. No hard choices. Unbelievable. Literally, unbelievable.

Politicians are often accused of being masters of "spin"—the rhetorical device that enables conforming the truth to one's own advantage. No lies, just self-interest. This very human talent also has

very able practitioners among the budget and program offices of the federal government, who learn to fashion their budget presentations to advance the interests of their own department or agency. In this endeavor, there are two imperatives: to protect funding for existing programs, and to compete for new funding. In the face of polished department or agency budget presentations, it takes a critical, knowledgeable eye to pick up on embedded issues, to question program projections, and to enable sound judgments to redirect resources to more productive ends.

Accordingly, the national-level budget examiners must be at least as expert as the programs they are examining. And there we have a problem.

Where are such experts to be found? The people who are the "doers" usually don't want to be pulled back to serve as program and budget examiners, which many regard as tedious work. This is an enduring complaint and a problem associated with all centers: too many demands, too few capable people. As a consequence, it is very difficult to assemble review teams that can effectively evaluate the presentations from the component representatives. Repeatedly, I received second-hand after-action reports out of program and budget reviews, alleging that the information presented was misleading, or incomplete, or misdirected … but the reviewers either did not pick up on the deficiencies, or were not expert enough to challenge what they were told.

The strategic objectives established by the 2005 *National Counterintelligence Strategy* provided a framework for organizing and presenting existing CI plans and programs in a coherent way, but at least for the first budget year did not impose the discipline needed for course corrections or new starts to advance national strategic ends. More mature implementation planning may have supplied more precise measures to guide resource allocation, but given the inherent time lags of interagency coordination those plans would not be ready in time to meet the deadlines of the federal budget cycle. The good news is, all departments and agencies went through the drill of conforming their budgets to a national template, establishing a process which in later years may eventually yield a more coherent and

effective CI enterprise—provided their submissions are subject to informed and critical review.

4) Strategic operational planning. If there was one compelling requirement to emerge from the *post mortems* of the 9/11 attack, it is the need for strategic operational planning to tie together comprehensively what is known about terrorist threats with all options at home and abroad, acting alone or with allies, to defeat them. Among the many reviews, CIA's inspector general was especially direct on this point:

The Review Team found that Agency officers from the top down worked hard against the al-Qa'ida and Usama Bin Ladin (UBL) targets. They did not always work effectively and cooperatively, however. The Team found neither a 'single point of failure' nor a 'silver bullet' that would have enabled the Intelligence Community (IC) to predict or prevent the 9/11 attacks. The Team did find, however, failures to implement and manage important processes, to follow through with operations, and to properly share and analyze critical data… [114]

Despite the DCI's proclamation, "we are at war," and call for a full-out effort against terrorist threats, the inspector general specifically found that the DCI's Counterterrorism Center was not used as a strategic coordinator of the intelligence community's counterterrorism activities; rather its focus was primarily operational and tactical.

The Team found that neither the DCI nor [his Deputy] the DDCI followed up these warnings and admonitions by creating a documented, comprehensive plan to guide the counterterrorism effort at the Intelligence Community level. The DDCI chaired at least one meeting in response to the DCI directive, but the forum soon devolved into one of tactical and operational, rather than strategic, discussions…While CIA and other agencies had individual plans and important initiatives underway … no comprehensive strategic plan for

114 Executive Summary, June 2005, vii. Redacted version available at https://www.cia.gov/library/reports/Executive%20Summary_OIG%20Report.pdf,

the IC to counter [Osama bin Ladin] was created in response to the DCI's memorandum, or at any time prior to 9/11.[115]

> The lesson is straightforward. Where operations involving multiple agencies must be conducted to strategic effect, the executive branch must institutionalize national-level strategic operational planning and oversight. That requires representative elements from across the government with access to essential information, empowered to make decisions and to deliver results.

This compelling need is no less true for understanding and countering foreign intelligence threats than it is for understanding and countering terrorist networks.

In the six months leading up to Operation Iraqi Freedom, an interagency CI strategic planning team came together under Defense Department leadership to develop a common operating picture of Iraqi intelligence operations worldwide. In response to Command Authority direction, the team was chartered to develop CI operations to render Iraqi intelligence ineffective. While this effort, dubbed "Imminent Horizon," resulted in some important successes, the CI community learned its lessons the hard way. Strategic operational planning to degrade foreign intelligence capabilities has long lead times. Beginning at D minus six months—as was the case with Iraq—is too little too late. Even though Coalition Forces had technically been at war with Iraq for ten years, flying daily combat missions, the CI community could identify and contain an unacceptably low percentage of Iraqi intelligence personnel. The file folders were outdated, contradictory, and incomplete.

If the United States had such an inadequate picture of Iraqi intelligence personnel, who numbered among the nation's highest priority CI targets, imagine the intelligence gaps on foreign services of lesser concern.

Drawing on these and other lessons, the National Counterintelligence Strategy called for the establishment of a standing strategic

115 Ibid., viii

operational planning capability to proactively identify, assess, and defeat foreign intelligence threats. The Congress approved a pilot project for the Office of the NCIX to assemble strategic planners from across the community, along with the support infrastructure necessary to analyze candidate foreign intelligence services' capabilities and vulnerabilities. Working side by side with fellow planners from the several CI departments and agencies, they were responsible for developing collection strategies to fill in intelligence gaps and options to degrade foreign intelligence operations, consistent with larger national security policy objectives.

Beyond the Imminent Horizon experience, the NCIX pilot project was able to draw on the intensive focus on strategic operational planning by its sister DNI organization, the National Counterterrorism Center (NCTC). The morning-after lessons of 9/11 had resulted in legislation creating the NCTC, and specifically assigning the NCTC the duty to conduct strategic planning for the U.S. government's counterterrorism operations. As NCTC's first Director Scott Redd explained, strategic operational planning "serves to fill a long existing gap in government….

Simply put, the White House, in the form of the National Security Council and, more recently, the Homeland Security Council, has been in the business of developing broad strategy and policy. At the other end of the spectrum, the Cabinet Departments and Agencies have been responsible for conducting operations in the field…What has been missing is the piece in between policy and operations, a concept not unfamiliar to the military…Strategic Operational Planning is designed to fill that gap.

The goal of strategic operational planning is straightforward: to bring all elements of national power to bear on the war on terrorism in an integrated and effective manner.[116]

NCTC has struggled with this part of its charter, in part because strategic operational planning to identify and neutralize terrorist

116 John Scott Redd, Statement for the Record before the House Armed Services Committee, 4 April 2006, available at http://www.nctc.gov/press_room/speeches/20060404.html.

threats must draw on government resources that extend well beyond the intelligence community. The line where NCTC responsibilities end and those of the Defense Department's internal planning processes begin is especially difficult to define.

By contrast, strategic operational planning for counterintelligence should be easier to deliver, since no department or agency has claimed lead responsibility for the mission of defeating foreign intelligence threats—a void highlighted by our experience in the Iraq war. Even so, the congressionally approved CI strategic planning pilot project ran into stiff resistance, especially from CIA, which is straining to meet all of the extra staffing requirements imposed by the numerous new DNI centers, directorates and mission managers.

Perhaps owing to CIA's reticence and doubtless for other reasons as well, my successor as NCIX terminated the pilot project, and assigned the group's resources and related mission to the new National Clandestine Service. That assignment begs the question whether the National Clandestine Service can do this job—even assuming that it wants to, which is far from clear. There are many reasons for concern, not the least of which is that the FBI, which is critical to effective strategic operational planning for counterintelligence, is not a part of the new service. And that is a serious problem.

The CIA, the FBI, and the military services are working in their separate channels to address different aspects of the foreign intelligence threat, with some important linkages between them; but bureaucratic resistance to ceding access to sensitive CI information—even the limited, sanitized information necessary to inform strategic direction—remains understandably fierce, if not always wise. It may be argued that the sorry history of successful, long-standing espionage carried out by trusted insiders is an indictment of the "each is responsible for its own house" approach to counterintelligence. Nevertheless, counterintelligence (and especially counterespionage) breeds an imperative to hold close to information, and to stay in control of these extremely sensitive operations and investigations. Indeed, if there has been one clear, consistent message from the field to the national centers, it has been "stay away from operations." Such a wall may be needed to preserve operational security and protect the lives and

missions of personnel at risk, but it becomes self-defeating if used to undercut insights and understanding vital to national coherence.

These ingrained obstacles to information sharing, along with uneven abilities among department and agency representatives to present much less task "blue" side CI resources, make the urgent job of strategic operational planning still one of the great undeveloped interagency arts. Fortunately, such reflexive protectiveness commonly is overcome in the field, where people with a shared duty station and purpose are clear that they are working on the same team. Without some way of instilling that spirit and incentive structure in Washington interagency planning groups, strategic operational planning for CI will remain an elusive goal. And the nation will continue to lack the means to integrate and orchestrate the government's CI activities to strategic effect.

In my view, joint operational planning is the key to transforming our nation's CI capabilities. The president can issue strategies, the interagency can table implementation plans, the budget examiners can have their say, but at the end of the day it is what the operators actually do against the adversary that will matter most. Strategic operational planning that enables well-orchestrated operations to degrade foreign intelligence threats would give the United States a formidable tool in protecting the nation's security and advancing our strategic interests. But in order to get there, the nation's CI organizations still face a steep learning curve.

Organizational Learning

During the time I served as NCIX, the CI community went through one full cycle, as envisioned by the Counterintelligence Enhancement Act, in which a) the president approved a strategy to guide the nation's CI effort; b) implementation planning was initiated to define the milestones on the way to meeting strategic objectives; c) current capabilities were baselined against those milestones; and d) a strategic operational planning cell was constituted to drive the integration of U.S. CI activities to common ends.

And then it was Groundhog Day.

In 2007, a new *National Counterintelligence Strategy* was issued, with a different set of strategic objectives to be implemented. On its face, the

new document was not inconsistent with the first strategy, but it was different especially in its low-key treatment of the proactive strategic operational planning that was the centerpiece of its predecessor. Current CI budgets and programs would need to be baselined against different milestones. As the system reset to the starting position, the federal budget cycle pressed ahead, individual department and agency activities continued apace, and the NCIX-led effort to integrate the nation's diverse CI activities was left on the sidelines, running to catch up—not an ideal posture from which to lead.

I fear the generic lesson the CI bureaucracy learned from this experience was to do nothing, because soon there will be new national strategic guidance and new measures of effectiveness. In part, the new strategic guidance was a function of a change in leadership in the NCIX position (which is often a good thing, leading to a healthy interjection of new ideas). In part, the CI organizations got mixed signals from other officials in the office of the DNI, as the duties and authorities of the new intelligence architecture began to emerge. But there is also a dysfunctional rhythm and waiting game built into the system as presently conceived. By the time a new national strategy is written it is already too late to impact the allocation of resources. And then the process starts anew.

National strategy needs to have a half-life longer than 12 months. The law says that a national CI strategy must be issued every year; it does not say that this year's strategy must be different from last year's. The Counterintelligence Enhancement Act also charges the office of the NCIX with evaluating department and agency performance against the strategic objectives set forth in the *National Counterintelligence Strategy*. I hope the next NCIX will be able to turn to this important task before being obliged to write yet another strategy, in order to find a way to build on what has come before.

At the national level, enterprise-wide substantive organizational learning also comes from two other critical functions: the damage assessment process and after-action reports.

The lessons to be learned from espionage cases or other major compromises of national security information can be invaluable for supplying new insights to improve counterintelligence and security practices. The painstaking reconstruction of what happened and how

it happened, in order to identify the secrets that have been exposed (plans, programs, capabilities, lives) and the resulting damage to U.S. national security, is the compelling responsibility of the damage assessment team. The office of the NCIX has had some excellent people leading the damage assessment effort, and a well-oiled government process for conducting the reviews. Damage assessment teams draw their membership from across the government, and end up by salting the departments and agencies with personnel who have personal knowledge and experience with these sobering interagency investigations. Where the system still falls short is in the follow-through on recommendations for improvement, which is left largely to the discretion of the relevant department and agency heads. Of course, costly past mistakes are hard task-masters: it would be far better to be able to take action before our nation's security is put in jeopardy.

The after-action reports from Imminent Horizon (the CI campaign during the Iraq War) confirmed, once again, the compelling need for standing joint strategic planning, for building interoperability across CI agencies, and for proactive operations to degrade foreign intelligence threats. Participants across the CI community may disagree over the success realized by Imminent Horizon, but they all agree on the need for advance planning and preparations; for the future, it is a matter of having the discipline to do it. Even so, the pilot program for strategic operational planning at the NCIX has been shut down, as individual department and agency priorities and operational protectiveness took precedence over a national level planning effort.

A strong NCIX, empowered to function as a program director for the strategic CI mission including the ability to command resources, could follow through on strategic operational planning (and its necessary support structure) to ensure that we have the capabilities in place to defeat adversary intelligence operations. But here, the statutory scheme is wanting. It would take a later Commission to identify this key deficiency in the Counterintelligence Enhancement Act of 2002 and to recommend remedial action.

Beyond the Executive Branch: The Congress and the WMD Commission

The Congress drew on the thinking behind presidential order (PDD-75) and the work of an NSC-led review (CI-21) in creating the NCIX and committing the national CI mission to law. Once having created the NCIX, the oversight Committees had a vested interest in seeing it succeed. Here was a single office within the Executive Branch to be held accountable for all U.S. counterintelligence—an efficient mechanism to advance legislative oversight and other objectives.[117]

The NCIX became a favorite candidate for Congressionally Directed Actions (or CDAs, as they are known in executive branch shorthand), which for the most part was a good thing. Most department and agency action officers, while respectful of the authority and role of the legislative branch, regard CDAs as extra taskings that absorb time and energy and divert resources from other responsibilities. So CDAs, whether in law or in Committee Reports, are usually about as popular as taxes: unavoidable, but burdensome and unwelcome. By contrast, a small office with limited authorities, such as the office of the NCIX, may find CDAs very useful, because they can provide a vehicle for advancing standing goals and objectives.

As I recall, all of the CDAs that came our way were classified, so the specific taskings cannot be recounted here. Suffice it to say that some of the CDAs the Congress called on the NCIX to perform assumed powers and authorities not granted the NCIX, which as described above fell short of our job description. This was a problem in need of a creative solution. Consequently, in order to execute those CDAs (in consultation with the relevant congressional committees), we partnered with the cognizant inspector general (IG) to draw on his investigative and other authorities. These partnerships enabled us to require departments and agencies to produce documents and other

117 Earlier versions of the Counterintelligence Enhancement Act would have placed the office within the Executive Office of the President, which the administration opposed. The final act was a compromise, under which the NCIX reported to the president but the office administratively was under the DCI. Following the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004, the NCIX Office was made a part of the Office of the DNI and subject to his direction and control.

information, which proved very helpful in assessing some aspects of CI programs and performance. I do not believe all of the departments and agencies would have been so forthcoming without the power of the IG and the attention of the Congress behind the effort.[118]

There is a caution to this practice, however. The IG has a vital mission that includes conducting investigations for the purpose of assessing mistakes and determining fault. The IG's duty is very different from the job of providing strategic guidance to achieve coordinated objectives. A national office such as the NCIX cannot go to the well of IG powers too often without risk. It would undermine the ability of the NCIX to function were it to acquire a reputation among the several components as that of an organization engaged in second-guessing their actions rather than providing sound leadership.

In order to lead, coordinate, and integrate U.S. CI activities, the NCIX needs visibility into those activities, and the ability to direct changes as required. But the Counterintelligence Enhancement Act, while assigning specific duties to the NCIX, does not give the NCIX directive authority over the CI elements; nor does it impose a corresponding duty on the elements of the CI community to support the NCIX. One might hope that the departments and agencies nevertheless would be forthcoming in supporting the national mission; unfortunately the exceptions tend to outweigh the rule.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, constituted to examine U.S. intelligence in the wake of major failures in the lead up to the war with Iraq, also devoted substantial attention to the problems of U.S. counterintelligence.[119] Its report was a strong validation of the NCIX

118 Despite the mandate of the NCIX to head U.S. counterintelligence, the several CI departments and agencies reserved the right to withhold information they deemed "ORCON" (originator controlled). Among other difficulties, this resulted in my attendance as the head of U.S. counterintelligence at a Senate hearing on the FBI's handling of the Hanssen espionage case at which I was the only person in the room not given access to the document under discussion. (This confusion was later resolved but not in time to keep us all from looking a little silly.)

119 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("WMD Commission") Laurence H. Silberman

mission, and called for a fully empowered NCIX. "To make this more than window-dressing," the Report added, "the NCIX needs all of the DNI's authorities for counterintelligence," including the directive authority noted above.

Finding that "the United States has not sufficiently responded to the scope and scale of the foreign intelligence threat," the judgment of the commission was unequivocally in support of building a strong strategic CI capability and going on the offense. It cited with approval the proactive orientation of the National Counterintelligence Strategy, which the president approved as the commission's report was going to press, but added a caution that reinforces one of the key concerns of the Project on National Security Reform:

> But a new strategy alone will not do the job. As in the old – and clearly unsuccessful – approach to homeland security, U.S. counterintelligence is bureaucratically fractured, passive (i.e., focusing on the defense rather than going on the offense), and too often simply ineffective.[120]

Accordingly the Commission made a series of major recommendations, starting with the empowerment of the NCIX and calling on CIA, FBI, and DOD to undertake specific initiatives that collectively would re-engineer U.S. counterintelligence to enable centrally directed strategic CI operations.

Overall, the commission's review of the intelligence community's performance was devastating: "We conclude that the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction. This was a major intelligence failure."[121] But its conclusions concerning counterintelligence validated the major objectives established by my office and the new National Counterintelligence Strategy. The commission's specific recommendations were endorsed by the president, and the principal deputy DNI established a

---

and Charles S. Robb (Co-Chairmen) *Report to the President of the United States*, March 31, 2005; see especially Chapter 11.

120 Ibid., 487.

121 Ibid., transmittal letter from the co-chairmen to the president (cover page).

record of accounting to measure progress in implementing those recommendations.

It would be difficult to find a clearer expression of national guidance than the combination of congressional support, a consolidated national strategy, the consistent findings of a highly respected commission, the president's embrace of its recommendations, and a running score card on their implementation. By any measure, the statutory NCIX mission to lead and integrate U.S. counterintelligence was well positioned to succeed. Nevertheless, that clarity of purpose proved insufficient to navigate the well-entrenched institutional obstacle course.

Corporate and Individual Personalities: The Office of the DNI

The need for U.S. intelligence to be integrated and centrally directed was obvious from the outset, which was why the DCI was created sixty years ago to provide central guidance and ensure coordinated action. Even so, the decades of experience since the National Security Act of 1947 have been a testament to the difficulty of implementing these goals, as the ongoing struggles of the Office of the Director of National Intelligence illustrate.

The arguably even greater hurdle of imposing a chief executive, sixty years after the fact, to lead an assortment of heretofore autonomous, disconnected, and vastly different CI agencies is impressive in the annals of organizational reform. As with many national-level programs, the good government principle is to know where to draw the line to establish necessary centralization while preserving the freedom of action (including the responsibility, accountability, and authority that come with that freedom) essential to success. It helps, however, if the several CI components and the national leadership have the same end goals in mind. I fear they may not.

Nowhere was this disparity of view more salient than in my relationship as the NCIX to the front office of the DNI.

The establishment of the DNI was a declaration that the intelligence community needed a more powerful center. The DNI inherited the authorities and responsibilities of the Director of Central Intelligence, with what the Congress intended as more clout, not burdened by the

added responsibility of running CIA. The DNI was also assigned some new and expanded duties, such as directing the explicit missions of the National Counterterrorism Center and the NCIX.

The original Counterintelligence Enhancement Act was careful to make the NCIX independent of the Director of Central Intelligence. This reflected the Congressional view of the breadth of the national CI mission and its objective of removing counterintelligence from its past second tier status within the intelligence community. But as our experience would show, the NCIX did not have the authorities needed to accomplish the mission she was assigned.

The NCIX is the head of U.S. counterintelligence, but does not have the power to direct U.S. counterintelligence. Before the creation of the DNI, there was no ready solution to this problem short of changing the law. The new architecture of the intelligence community seemed to be precisely what was needed to bolster the national CI mission as well.

I was an early advocate of moving the NCIX under the office of the newly created DNI, which I thought would prove an enormous boost to fledgling national CI mission. Among the powers and authorities inherent in the head of U.S. intelligence are powers and authorities over the great majority of the programs and activities that make up U.S. counterintelligence, which has an analytic component, and a collection dimension, and a unique operational focus. I expected that the DNI would turn to the NCIX to execute these powers and authorities over counterintelligence, under his direction and control.

The WMD Commission was of a like mind. In the course of fulfilling its original mandate to examine the performance of U.S intelligence in the Iraq war, the commission was asked to develop a blueprint for the new office of the DNI. In its review of counterintelligence, the commission concluded that the national CI mission could not succeed under the limited grant of authority to the NCIX.

To remedy this deficiency, the commission expressly recommended that the NCIX be empowered with the DNI's authorities over U.S. counterintelligence, including in particular his tasking and budget authorities.

The DNI chose a different path. As mentioned above, the deputy DNI for management was delegated all of the DNI's authorities over the budget, including the CI portion. The effects of this decision on the ability of the NCIX to guide CI budget allocations quickly became clear. As part of a larger effort to pool funds that could be made available to meet high priority needs, my office was asked to identify the bottom 3 percent funding for U.S. counterintelligence. But when the report was prepared, the deputy DNI's office substituted their evaluation for our recommendations, which the DNI affirmed without discussion. Also as part of a larger effort, my office was asked to evaluate what part of U.S. CI funding should be funded under the National Intelligence Program (the consolidated intelligence budget for which the DNI is principally responsible), rather than the Military Intelligence Program, which is under DOD control. Again, the Office of the Deputy DNI for Management substituted their evaluation for our recommendations, which the DNI affirmed. The several CI components drew the obvious conclusion.

Similarly, the deputies for collection and analysis were delegated all of the DNI's authorities in their respective areas, including the DNI's tasking authority over CI collection and analysis. In an especially candid meeting, the deputy head of the CIA's directorate of operations told me that his office was coordinating all CI collection matters with the deputy DNI for collection, and specifically not with the NCIX, per her direction. It is difficult to understand how the statutory charge to the NCIX to set CI collection and analytic priorities can be squared with a DNI organization that allocates these duties elsewhere.

The Congress had placed the NCIX under the president and not under the DCI precisely to keep the national CI mission whole and apart from the intelligence stovepipes. Instead of protecting this careful consolidation of national leadership when the NCIX was brought under the new DNI, the old model of functional divides, with its old problems, resurfaced. Counterintelligence was subordinated within the larger intelligence mission, strewn like the Scarecrow across several power centers of the office of the DNI. The pendulum was moving back, contrary to the objective of the Counterintelligence Enhancement Act, which envisioned consolidating all CI responsibility in one place under a single national leader.

The unique responsibility of the NCIX is to bring CI options to the policy table, and to translate national security policy objectives into counterintelligence imperatives. In order to do this, the NCIX must be fully integrated into the pesident's national security team.[122] It is of course also essential that the NCIX be a trusted member of the DNI's core management team; but it was critical to the stature and nature of the job that the NCIX was appointed by the President. Unfortunately, a technical conforming amendment, integrating the Counterintelligence Enhancement Act into the Intelligence Reform and Terrorism Prevention Act, subordinated the NCIX to the DNI's appointment authority, effectively downgrading the position. My recommendation to seek reinstatement of the president's appointment power was not supported by the DNI.

Other DNI decisions resulted in further fragmenting U.S. CI funding, complicating efforts to coordinate CI plans and programs. Substantial parts of the DOD's CI budget, formerly funded under the National Intelligence Program, were moved into the Military Intelligence Program over the objections of the DOD program manager and the NCIX. To make matters worse, substantial parts of the FBI's intelligence budget (the lion's share of U.S. counterintelligence) were also moved out of the National Intelligence Program, also over

122 I would like to interject a personal note on my selection as the NCIX. In the course of my career, I had broad policy experience in national security strategy including in particular counterintelligence policy and related laws, but I did not come up through the ranks of CI or intelligence professionals. Instead, I came to the position as a political appointee—one of only a handful in the intelligence community. Indeed, as I looked around the table at the DNI's senior staff meetings, I was the sole participant who was not a career civil servant (including the DNI himself, John Negroponte, who had a long and very distinguished career in the State Department where he now serves as the Deputy Secretary). I believe that my status as an intelligence community "outsider" may have led to some distance between myself and other senior members of the DNI's organization, who had been handpicked by the DNI. But I also believe this personal background gave me a twofold advantage as the NCIX. I was not viewed as biased in favor of any particular department or agency's approach to counterintelligence because I neither came from nor expected to return to a career service position. And I was able to interact effectively with other members of the president's national security leadership team because I had come into office as a part of that team—which I believe was crucial to my effectiveness as NCIX.

NCIX objections.[123] It may be that some of these decisions reflect compromises between the DNI and cabinet secretaries on larger intelligence budget questions. But the net result was that almost half of U.S. CI programs and activities formerly funded under the national intelligence budget were farmed out to department and agency control—a sharp move away from central strategic direction of U.S. counterintelligence.

Other actions taken by the DNI front office also undercut the statutory responsibilities of the National Counterintelligence Policy Board to advise the president on key policies and procedures impacting U.S. counterintelligence. The new National Clandestine Service, which consolidated Defense and CIA HUMINT, explicitly includes an interagency CI staff—which was presented to the NCIX and the Policy Board as a *fait accompli*. But what was the purpose of this new CI office? How was it to be resourced? In response to a request from the Defense Department, I called a meeting of the board to evaluate the roles and responsibilities of this new national CI element. But that board meeting never took place. The CIA representative, who was to brief the board on the new service, called to say that he had been instructed by the DNI front office not to attend (presumably to wall-off planning for the new clandestine service from Policy Board purview). Without the CIA briefing, there was nothing to discuss so the meeting had to be cancelled. It was regrettable, to say the least, that the DNI's chief of staff would concur in the decision to call a Policy Board meeting one day but secretly countermand it the next. It was even more regrettable that the Policy Board never had the opportunity to consider the relationship between the CI element within the new National Clandestine Service and the larger implications for U.S. counterintelligence.

If the DNI had implemented the WMD Commission's recommendation to empower the NCIX, we still wouldn't have a bed of roses on the road to transforming U.S. counterintelligence. The centrifugal forces protecting legacy divisions of responsibility

123 I later learned that our memo assessing the FBI's CI budget structure within the larger national context and providing NCIX recommendations to the DNI had been "lost" by the front office (both the hard and soft copies) and never made it to Ambassador Negroponte's desk.

and other impediments to national integration are and would remain formidable, as discussed throughout this case study. But many of the difficulties we encountered in moving the CI enterprise to carry out the strategic CI mission would have been significantly lessened.

Unfortunately, the DNI front office placed a higher priority on consolidating its own power first. As a result, the DNI's substantial CI-related authorities were vested in the several deputies, mirroring the old DCI community management staff and creating in effect competing power centers within the DNI organization. By purposeful decision by the DNI and his senior advisors, the NCIX organization has been limited to the powers and authorities granted in the law that first created it, which the commission concluded is a recipe for failure.[124]

Collectively these actions by the DNI front office would appear to reflect a far different view of the role and purpose of the NCIX than that advanced by the WMD Commission, and I fear that if left to stand, they are likely to deepen the already difficult challenge of bringing strategic direction to U.S. counterintelligence. Without clear and effective central leadership, the several CI components will naturally look first to their legacy responsibilities rather than the new challenges that the strategic reorientation of the Nation's CI enterprise would impose.

Outcomes

When I left office, the starting blocks for a new strategic CI capability were in place. In line with the WMD Commission's recommendations, the new National Clandestine Service, unifying HUMINT services under the CIA, is ideally situated to deliver, for the first time, a genuine CI capability abroad to complement the FBI's responsibilities

124 On a positive note, last year the DNI designated the NCIX the "mission manager" for CI, which assigns some of the DNI's authorities over counterintelligence to the NCIX. Unfortunately this is only a partial solution, because "mission managers" (which have also been established for counterterrorism, counterproliferation, North Korea, Iran, and Cuba/Venezuela) are subordinate to the three DNI deputies for management, analysis and collection, meaning that CI authorities and responsibilities still remain divided among the DNI deputies.

at home. The consolidation and enhanced professionalization of all of the FBI's national security functions under the new National Security Branch should enable a more systematic and strategically driven approach to the bureau's intelligence mission including its CI work. The Defense Department's strategic CI orientation has been institutionalized in the mission of Counterintelligence Field Activity and the ongoing work on CI campaign plans now incorporated within the Department's deliberate planning process. And with the issuance of the 2005 National Counterintelligence Strategy, the office of the NCIX engaged the CI community to build central data bases on select foreign intelligence services to support strategic analyses and to identify collection needs, and established a pilot project for a CI community integration center to conduct strategic operational planning to degrade foreign intelligence capabilities.

Yet despite these accomplishments, the ability to execute strategic CI operations remains a far-off goal. In fact, if we had to issue a scorecard today, the results would be quite discouraging.

It is uncertain whether plans for the new external CI cadre at the CIA will survive in the face of competing demands on the agency's HUMINT collection and other clandestine resources. The FBI's performance in shouldering the national security responsibilities it has been assigned is the linchpin to executing the strategic CI mission; but as both the WMD Commission and the 9/11 Commission cautioned the FBI's past record in effecting institutional and cultural reform to address transnational security threats is not encouraging.[125] At the Defense Department, the Counterintelligence Field Activity has seen its budget sharply curtailed, and as of this writing its future is highly uncertain.[126]

125 "WMD Commission," *op cit*. See Chapter 10 citing the 9/11 Commission's findings. The chorus of skeptics is growing louder (sparked in part by concerns over the FBI's exercise of its authority to issue National Security Letters). See, e.g., Richard Posner, "Time to Rethink the FBI" *Wall Street Journal* March 19, 2007, A13—the latest in a continuing critique by Judge Posner. For a reply, see Louis Freeh's letter to the editor, "Former FBI Director Says U.S. Doesn't Need a National Police Force," *Wall Street Journal*, March 31, 2007, A9.

126 Mark Mazzetti, "Pentagon is Expected to Close Intelligence Unit," *New York Times,* April 2, 2008.

Within the Office of the DNI, authorities and lines of responsibility for counterintelligence are blurred, diluting the concentrated focus and guidance that the NCIX was created to provide and that the WMD Commission insisted it must have. Despite the work of the new national organizations under the DNI and the subordinate office of the NCIX, the unity of effort and priority requirements of strategic CI have yet to find expression in ordering the plans, programs, budgets, or operations of the component CI agencies. Rather than building on the first *National Counterintelligence Strategy*, the next iteration established a new set of performance criteria, making it impossible to get ahead of the budget cycle. And the seminal strategic operational planning needed to enable coordinated proactive operations against foreign intelligence targets at best has been deferred.

Lingering questions over the core mission of the NCIX. Overall, the most formidable obstacle to progress has been the lack of understanding or consensus behind the purpose and value of strategic counterintelligence itself, which has led to confusion over the central mission of the NCIX. Is the goal to establish a new national capability to execute a new strategic CI mission? Or is it simply to become more efficient at performing the standing missions of the several CI agencies?

While the goal of establishing a new strategic CI capability would be transformational, the alternative goal of improving the efficiency of the existing CI enterprise may be illusory. The first goal requires genuine integration and central orchestration of CI activities across the government (a focus of the Project on National Security Reform). The second assumes that adding another layer of bureaucracy can supply the means for increasing efficiency—a risky proposition at best.

The ambiguity over the true mission of the NCIX lends itself to different measures of effectiveness for the office. I believe the right answer—and the answer one would hear from Congress and the authors of CI-21—is that the NCIX should be measured by its success in building a strategic CI capability for the United States. A genuine strategic CI capability would have value in its own right as a tool of national security planning and execution. It would also serve as the driver by which all U.S. CI activities would be enhanced, given the inherent tactical advantages of strategic dominance.

I fear that the standards being applied to the NCIX derive from the subordinate goal of overseeing the efficiency of the existing CI enterprise. Key decisions by the DNI's office concerning NCIX resources and grants of authority have been inconsistent with what is needed to establish much less execute the strategic CI mission. And the office of the NCIX has been assigned other non-CI duties (including in particular security-related responsibilities for acquisition risk assessments and technical security countermeasures programs), while its impact on U.S. counterintelligence has been negligible.

This suggests an interesting paradox. Is it possible to set expectations too low for a national mission to succeed? If the job of the NCIX is simply to make sure that the CI departments and agencies are performing efficiently, he or she may well fail, because there may be little a central office can do to improve the efficiency of the existing disaggregated business model of U.S. counterintelligence. If the resulting marginal increase in efficiency is negligible (or negative), the experiment in central CI leadership may be deemed a failure.

If by contrast the job of the NCIX is to create a new strategic CI capability for the United States, then the law creating the NCIX fell short of the mark. It established a new head for counterintelligence, but carefully denied the NCIX any directive authority over counterintelligence. How can the NCIX "head" national counterintelligence but have no power to direct? Guidance from such an executive is inherently advisory, rather than authoritative. One can be an advisor to a line manager, but to be an advisor to a bureaucracy makes no sense. U.S. counterintelligence does not need an advisor, it needs a leader.

What accounts for this fundamental design flaw? Perhaps the Congress (and the preceding CI-21 review) wanted to have it both ways: to create a new head of U.S. counterintelligence without detracting from the powers of the several cabinet heads with CI responsibilities (especially the FBI). Such hedging may be simply the undesirable consequence of compromise leading to a substandard result. But it may also reflect a prudent caution not to transfer real power to an untested new organization, in an attempt to honor the "first do no harm" principle in imposing a new solution (the NCIX) to solve an old problem (CI weaknesses). I fear, however, that harm is

done nonetheless when history tests the solution and finds it wanting, missing the point that the failure was more in its design than its execution.

The problem with "czars." At another level, the difficulty we encountered in moving from national strategy formulation to execution is not unique to counterintelligence. In my experience, it is in fact possible to integrate across departments and agencies; but there are some vital characteristics of the integrating mechanisms that must respect both the limitations and the possibilities inherent in how the government works, starting with the problems of the "czar" model.

National "czars" have a number of common features, and have experienced common frustrations. First, their resources are largely derivative, and their functions are mainly to coordinate, integrate, and guide. So by definition, they are in competition with other department and agency priorities.

These national missions cannot succeed unless cabinet departments and agencies have an obligation to support them. We almost always miss this part in creating czar-doms. The problem is not so much a matter of bureaucratic hierarchy (who gets to call the shots). Rather it is a need for a common obligation to be levied on all relevant department and agency heads to achieve the national mission as a mutual goal and responsibility. It should be part of their personal measures of accomplishment whether that national goal succeeds—as well as their statutory duty.

Second, in place of line authority, czars depend on having the support of the president and a bully pulpit for exhorting departments and agencies to act. The president has vast responsibilities and his time is precious and rare. As a result, national czars with vital missions are very much on their own, which means they need independent sources of power. And that is a problem.

I suspect the czar model does not work well in our democracy in part because Americans rebel against the over-concentration of power in one place. Cross-cutting national missions are important—but they do not operate in a vacuum. They are one among many national objectives that must compete for resources and priority attention. Broad objectives of integration and coordination are best

accomplished not through promulgating guidance (as essential as that is), but through discrete national activities or programs that enable supporting activities to conform to their requirements.

In other words, effective integration and coordination across the interagency requires the discipline of a national program: the budgets, billets, authority, and accountability to meet defined ends. It is not enough to exhort cooperation through national guidance or interagency meetings. Even strong national leadership, charismatic personalities, and popular ideas will falter absent the institutional tools that drive, capture, and internalize the results needed to enable strategic coherence.

The Counterintelligence Enhancement Act of 2002 filled the biggest hole at the center of the national CI system. It established the NCIX as the head of U.S. counterintelligence, and gave shape to a new national CI mission. However, while charging the NCIX with that mission, the act did not create a national strategic CI program that the NCIX would be empowered to manage. In other words, it created a national executive but not the means of execution.

As a result, we have a national CI strategy, but we do not have a national CI strategic capability. National strategies are not real unless they connect means to ends and means are only connected to ends when people are held accountable for employing the resources they control to achieve those ends. Again, these are the qualities of a program. And they are qualities the national counterintelligence mission does not yet possess.

Still there is reason for optimism. The very existence of a national office changes the federal landscape. Having stepped away from the daily demands of the NCIX job, I have come to see that the path ahead for U.S. counterintelligence, while far from certain, is at last clearly marked. Inevitably there will be greater coordination across U.S. CI activities as the departments and agencies factor national-level expectations into their daily work and future plans. It is also valuable for the rank and file doing the challenging work of counterintelligence to know they have a national-level advocate for what they do. But this is far short of what we set out to accomplish. And failure carries a heavy cost.

The Dangers Ahead. In recent history, the United States has sustained stunning losses to foreign intelligence services, which penetrated through espionage and other means virtually every one of the most secret, highly guarded institutions of our national security apparatus. Any one of these major compromises could have had devastating consequences in war. Now that we are at war, the potential consequences of intelligence and other critical information compromises are more immediate, placing in jeopardy U.S. operations, deployed forces and our citizenry. And with U.S. forces in Afghanistan and Iraq, and American intelligence and special operations teams pursuing Al Qaida networks worldwide, traditional adversaries of the United States, as well as some new ones, see a window of opportunity, and they are seizing it.

Most of the world's governments now have some kind of standing external intelligence service, including an impressive number that are highly capable and organized, trained, equipped, and deployed directly against the United States and our interests. Their numbers are growing in absolute terms, and growing relative to ours and especially relative to the resources we have dedicated to counter them. Today's chief intelligence adversaries are disparate in their structures, diverse in their operations, working within society more than under embassy cover, and learning from one another.

The work of clandestine services, engaged in intelligence collection and other activities, is an arena of international competition where the advantage does not necessarily go to the rich or the otherwise powerful. Foreign adversaries may not have a prayer of fielding costly and technologically demanding technical collection suites (and the U.S. government has worked very hard to keep it that way), but they can organize, train, equip, sustain, and deploy impressive numbers of case officers, agents of influence, saboteurs, and spies. And they do, in numbers commensurate with their value.

As these intelligence services expand their skills and reach, the United States has become the single most important collection target in the world. From the standpoint of foreign intelligence interest, there are many potentially valuable targets outside of our borders, such as U.S. forces abroad and the far-reaching activities of critical American commerce and industry. But the real intelligence treasure trove for

foreign powers is here in the United States, where the opportunity for intelligence officers and their agents to move about freely, develop contacts, and operate in the dark is no more lost on foreign intelligence adversaries than it was on the nineteen hijackers that September morning.

The United States has been slow to appreciate the effects of these intelligence operations, much less to address the threats they pose to current U.S. foreign policy objectives or enduring national security interests. We know surprisingly little about adversary foreign intelligence services relative to the harm they can do, or relative to the insights to be gained by analyzing the distinctive ways in which they operate, and the different purposes they serve. And U.S. capabilities to disrupt, degrade, or exploit the intelligence operations of potential adversaries remain woefully inadequate to answer that call.

The National Counterintelligence Strategy of 2005 directed a strategic reorientation of the nation's counterintelligence enterprise to confront these growing threats proactively. To this end, the strategy mandated the integration and central orchestration of the Nation's CI activities to identify and assess foreign intelligence threats to the United States, identify gaps in our knowledge and collection strategies to fill those gaps, and plan and execute strategic CI operations as national security priorities dictate. The national security leadership has every reason to expect that the CI community is hard at work to be able to deliver that new strategic CI capability. Without substantial change, I fear they may be disappointed.

Conclusion

The core questions posed at the outset of this case study asked four things: Can the U.S. government develop real strategies, and if so can it then implement them? If not, why not, and how much does that failure cost us? Here are some answers, along with some ideas for improvements.

In establishing the NCIX, the U.S. government recognized the need to integrate U.S. counterintelligence to strategic effect. The first National Counterintelligence Strategy articulated strategic objectives and the WMD Commission recommended specific new initiatives to enable

strategic operations. Taken together, these U.S. government initiatives, one from Congress, one from the president, and one from an independent commission, set forth consistent and clear new strategic direction for U.S. counterintelligence.

The execution of the national CI mission is entrusted to the NCIX, whose office was created expressly for the purpose of bringing strategic coherence to U.S. counterintelligence. Getting the departments and agencies to work together, however, thus far has proven an elusive goal. The difficulties range from the unique history of the disaggregated U.S. CI enterprise, to deficiencies in the NCIX and DNI organizations, to a seeming lack of awareness of the gravity of foreign intelligence threats among our national security leadership.

For U.S. counterintelligence, the steps mandated by the Counterintelligence Enhancement Act are only a partial answer. The law established a national leader to bring strategic direction to U.S. counterintelligence, but failed to establish a strategic counterintelligence *program*. While giving the NCIX all-encompassing responsibility for heading counterintelligence, the law failed to assign the NCIX even the minimal authorities commensurate with those of a program manager for the strategic CI program.

Program and budget authorities for CI activities essential to national objectives remain divided among the departments and agencies and subject to their individual priorities. Under this old business model, we are getting about the best we can expect out of our CI programs. Without the power of a common purse and the discipline of a national program, the mission of integrating and redirecting U.S. counterintelligence to achieve strategic cohesion may well be impossible.

Seven years after the NCIX was created, no single entity has a complete picture to provide warning of possible foreign intelligence successes, to support operations, or to formulate policy options for the president and his national security leaders. This compartmentalization of information is another reflection of the lack of a common set of principles or doctrine across the CI profession, which is defined more by the differences between its several components than by their commonalities. While bilateral interaction among the five operational agencies of the FBI, CIA and the military

services has increased in recent years, taken together those contacts do not begin to equal a cohesive, integrated whole.

Study after study has documented the high cost we pay for these seams in U.S. counterintelligence. Especially now, in the aftermath of 9/11, there is no excuse for allowing this dangerous incoherence to persist. For the future, avoiding strategic CI failure will require more than simply doing more of the same.

Recommendations. If the United States is to have the ability to integrate and coordinate CI activities to strategic effect, there are four core imperatives for change.

First, while tactical execution must remain with the responsible agencies, there should be a national program for strategic counterintelligence, with dedicated resources at the national level and as assigned among the executing departments and agencies, to identify, assess, neutralize, and exploit high-priority foreign intelligence threats to the United States. Specifically, the several departments and agency heads who oversee CI operational components should be directed by law or presidential order to configure their organizations to support the strategic CI program. The national program should comprise the specific components at the CIA, the FBI, and the military services, as well as the dedicated elements within the Office of the DNI.

Second, we do not need big new bureaucratic structures that take people away from the field; but as part of the strategic CI program, an elite national CI strategic operations center, manned and empowered by the constituent members of the CI community, should be established to integrate and orchestrate operational and analytic activities across the CI community to strategic effect. With the support of the center, the DNI/NCIX could supply additional insights and options for policy makers to achieve national security objectives, and translate national security policy priorities into strategic CI effort. With the production of CI options to bring to the policy table, it would be a simple matter for the standing national security decision making process to integrate CI into broader national security strategy and planning.

Third, housing the NCIX under a strong Director of National Intelligence (DNI) should have been a boon to the national CI

mission; instead the DNI bureaucracy has become part of the problem as CI responsibilities have been dispersed across the DNI organization. As the WMD Commission recommended, the NCIX office should be revalidated and empowered to perform the mission it has been assigned. In particular, the Director of National Intelligence should delegate his directive authority over CI budget, analysis, collection, and other operations, to the NCIX, which would go a long way toward empowering the national CI mission with the authorities and resources it must have to succeed.

Finally, we need to educate our national security leadership to the importance of counterintelligence as a tool for national strategy. While the manner in which adversaries may use intelligence to advance their interests and prejudice our own may not be an unfamiliar concern, what U.S. counterintelligence can and should do about those capabilities too rarely is addressed as part of national security policy and strategy. Including counterintelligence as part of the core curriculum in national security studies programs at our nation's war colleges and private universities would be a grand place to start.

During my time in office, it was my privilege to witness the extraordinary achievements and dedication of America's counterintelligence professionals. In having the high honor of leading that community, I came to understand the true potential for counterintelligence as a strategic instrument of statecraft. I also saw the terrible costs of legacy practices that divide rather than unite our community, to the detriment of our common mission. I hope that the insights gained through the Project on National Security Reform can be imported into the often-neglected realm of U.S. counterintelligence, to the betterment of our nation's security.

Appendix B: Appendices to "The NCIX and the National Counterintelligence Mission: What Has Worked, What Has Not, and Why"

APPENDIX B1: OPTIONS FOR DESIGNING THE NCIX OFFICE (JUNE 2003)

CORE PURPOSE	FOCUS	KEY FUNCTIONS	PRODUCTS	LEAD CUSTOMERS	REQUIREMENTS OF NOTE
Macro risk assessment to support protection measures	National level risk assessment, broad policy development	Assess what is of value Assess vulnerabilities, Assess risk, Propose mitigation strategy	Catalogs, data bases, National Security Threat List validation, Reports to Congress	Congress Public	Broad public outreach, Contractor support
Grand strategy	Defeating adversaries; defensive & offensive operations	Analyze strategic purpose of select foreign intelligence services, Develop strategic approach to defeat, Develop strategies to exploit knowledge of adversary's objectives	Reports to select Policy Coordinating Committees, Actionable CI Operational recommendations	NSC members and subordinate offices, NSC interagency groups, Operational units	Sophisticated foreign policy & area expertise, Linkages to sensitive operations

Central CI analytic brain	Exploit vast intelligence collection to support real CI analysis	All source CI macro-analysis, Eclectic integration of intelligence, CI reporting, other information to discern anomalies, patterns, markers	Analyses, Damage assessments, Warning to affected national security elements and security managers	National security community, Security managers	Experienced & creative analysts, Wide & deep access to intelligence reporting, Surge capability
Integrator of CI activities government-wide	Processes to improve CI analysis & operations	Identify issues for CI concentration Direct/facilitate issue-specific analytic centers Focus on processes	Designation of lead issues, Integration modalities, Damage assessment integration	Key CI departments & agencies	Authority or leverage to effect integration, Insight to be able to identify opportunities for improvements
Precursor to national CI service	Organization and Measures of Effectiveness for U.S. CI	Develop common training, standards, professionalization of CI service Examine policy/legal implications Develop and implement pilot project	Requirements study: Cost/ benefit analyses, Implementation plan, Charter, Concept of Operations, Draft NSPD, Legislative package	DCI, AG, FBI Director, SECDEF, Homeland Security Secretary, CI professionals, Congress	Board of advisors, Blue ribbon studies, FBI support

APPENDIX B2: NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES

Preface

The Counterintelligence Enhancement Act of 2002 (50 USC 401) directs that the Office of the National Counterintelligence Executive produce, on an annual basis, a strategy for the counterintelligence programs and activities of the United States Government. This is the first *National Counterintelligence Strategy* promulgated pursuant to that Act. President George W. Bush approved this *National Counterintelligence Strategy* on March 1, 2005.

Counterintelligence, as defined in the National Security Act of 1947, is "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities."

As used in this *Strategy*, counterintelligence includes defensive and offensive activities conducted at home and abroad to protect against the traditional and emerging foreign intelligence threats of the 21st Century.

Introduction

The National Security Strategy of the United States seeks to defend the peace by fighting terrorists and tyrants, to preserve the peace by building good relations among the great powers, and to extend the peace by encouraging free and open societies on every continent.

These fundamental objectives of our great Nation are not easily won. The terrorists and tyrants, the opponents of peace and freedom, are not passively watching from the sidelines. They are actively engaged in efforts to undermine the United States and our allies, and these efforts include some dimension of intelligence activities directed against us. Specifically, foreign adversaries seek to:

- Penetrate, collect, and compromise our national security secrets (including sensitive information, plans, technology, activities, and operations) to advance their interests and defeat United States objectives.
- Manipulate and distort the facts and reality presented to United States policy-makers by manipulating the intelligence we gather, and by conducting covert influence operations.
- Detect, disrupt and counter national security operations including clandestine collection and special activities, special operations, other sensitive intelligence, and military and diplomatic activities.
    - Acquire critical technologies and other sensitive information to enhance their military capabilities or to achieve an economic advantage.
    - Collectively, these foreign intelligence activities present a threat to the Nation's security and prosperity. The United States requires national, systematic, and well- defined policies to counter them. A key to success in defeating these threats is a strategic counterintelligence response that supports the National Security Strategy.
    - *The National Counterintelligence Strategy of the United States* has four essential objectives:
    - Identify, assess, neutralize, and exploit the intelligence activities of foreign powers, terrorist groups, international criminal organizations, and other entities who seek to do us harm.
    - Protect our intelligence collection and analytic capabilities from adversary denial, penetration, influence, or manipulation.
    - Help enable the successful execution of our sensitive national security operations.
    - Help safeguard our vital national security secrets, critical assets, and technologies against theft, covert foreign diversion, or exploitation.

To achieve these objectives, we will draw upon the full range of counterintelligence capabilities including counterespionage, counter deception, and offensive operations against hostile intelligence activities. Each of these national security tools must be strategically driven and employed to protect the United States from foreign threats, and to advance our national interests.

This document sets forth the national counterintelligence strategy of the United States in the context of our broad national security objectives and the foreign intelligence threats we face.

Counterintelligence and National Security

America faces substantial challenges to its security, freedom and prosperity. To meet them we must defeat global terrorism, counter weapons of mass destruction, ensure the security of the homeland, transform defense capabilities, foster cooperation with other global powers, and promote global economic growth. Our ability to meet these challenges is threatened by the intelligence activities of traditional and non-traditional foreign powers. Foreign intelligence services and others (e.g., terrorists, foreign criminal enterprises, cyber intruders, etc.) use clandestine activities and operations to harm and disadvantage U.S. national security interests. Counterintelligence is a key strategic national security tool that we use to defeat these foreign threats.

I. We will extend the safeguards of strategic counterintelligence to the Global War on Terrorism.

During the Cold War, our adversaries gained access to vital secrets of the most closely guarded institutions of our national security establishment. These included the clandestine, technical, and analytic directorates of the CIA; the counterintelligence division of the FBI; sensitive National Security Agency operations; Naval intelligence operations; nuclear weapons information; cryptographic keys for our secure communications; operational war plans for the defense of Europe; and plans for ensuring the survival of United States leadership in the event of war.

These peacetime losses resulted in grave damage in terms of secrets compromised, intelligence sources and methods degraded, and lives

lost. Moreover, these compromises could have had even greater consequences had we been forced to go to war. Today we are engaged in a war on terrorism which has invaded our shores and threatens Americans around the globe. In this war, the potential consequences of counterintelligence failures are more immediate than during the Cold War, and put in jeopardy our combat operations, deployed forces, intelligence officers, diplomats, and other U.S. citizens.

Terrorists gain an advantage when they have the support of a state sponsor, which allow the intelligence services of these regimes to act as links to global terrorist networks. In Afghanistan and Iraq, we have seen limited examples where enemy intelligence operations have enabled terrorists to target Americans. In addition, Al Qaida and other terrorist organizations have employed classic intelligence methods to gather information, recruit sources, and run assets. In order to operate clandestinely, terrorist groups often act like intelligence organizations by conducting pre-operational planning, compartmented operations, covert communications, and training. The global war on terrorism requires an effective counterintelligence strategy to help counter these hostile activities.

II. U.S. counterintelligence will shift from a reactive posture to a proactive strategy of seizing advantage.

If the purpose of intelligence operations and analysis is to understand an adversary's plans and intentions, the purpose of counterintelligence is to be aware of and exploit the adversary's intelligence operations. We need to be aggressive and creative in exposing the activities of foreign intelligence services. Utilizing a proactive counterintelligence strategy can help identify specific intelligence collection techniques, and gauge an appropriate response to counter the interests of an adversary. This requires a tighter coupling between organizations that collect foreign intelligence, and counterintelligence organizations, in order to fully exploit collection, analysis, and offensive operations. We need to incorporate counterintelligence considerations into strategic and tactical planning, operations, and training. The Intelligence Reform and Terrorism Prevention Act of 2004, which created a Director of National Intelligence, with a National Counterintelligence Executive under the Director, takes a significant step toward increasing community-wide coordination.

Since 1985, nearly 80 Americans have been arrested for crimes related to passing classified information to foreign governments. These spies were able to operate undetected for too long with disastrous results.

- The Walker ring in the Navy – over 17 years
- The Conrad group in the U.S. Army – over 18 years
- The Ames case in CIA – over 7 years
- The Hanssen case in the FBI – over 21 years
- The Montes case in DIA – over 15 years.

Although each of these cases represents an individual success in terms of a criminal prosecution, taken as a whole they reveal a larger systemic vulnerability in our national security. In the past, a comprehensive focus was lacking in the intelligence community's approach to protecting secrets. The counterintelligence mission must be transformed into a more coordinated, community-wide effort to help neutralize penetrations of our government. Within the United States, we must transform both our operational and analytical focus from a case-driven approach to a more strategic assessment of an adversary's presence, capabilities and intentions. Strategic counterintelligence analysis must drive operations. This requires looking beyond customary targets, such as known intelligence officers, to a larger population of foreign visitors and others whose activities suggest they might be involved in intelligence collection activities against the United States.

III. U.S. counterintelligence will help protect the sensitive technologies that are the backbone of our security.

The U.S. national defense strategy is based on a continuous transformation that utilizes cutting-edge capabilities, and places a premium on sensitive technologies that provide an advantage. Plans that ensure strategic superiority can be jeopardized if essential secrets are stolen and incorporated into an adversary's weapons systems. The United States spends billions of dollars developing weapons systems, which often rest on essential technological secrets. If foreign intelligence services steal these technological secrets, both our resource investment and our national security advantage are lost.

Today, more than 90 countries target sensitive U.S. technologies. Many employ collection techniques that extend beyond simple clandestine operations, and include tasking visiting businessmen, scientists, foreign students, trade shows, and debriefing visitors upon their return home. Counterintelligence planning and execution must proceed from a national counterintelligence strategy and be an inherent part of the mission at research laboratories, defense establishments, and with partners in industry. Counterintelligence and security considerations should not be an afterthought imposed on scientists, researchers, and those who develop sensitive technology. Coordinated and integrated counterintelligence information and analysis will be made available to senior government leaders, and, when appropriate, to security managers in the private sector.

Comprehensive risk management, valid security practices, and an informed strategic worldview are among the best guarantors of success against foreign intelligence threats. We will reach out to the private sector, especially those in the science and technology community, to increase intelligence threat awareness by providing threat information, and educating these audiences to the variety of ways our adversaries acquire and steal information.

The departments and agencies charged with protecting the homeland are building new channels for information sharing across government, including at the state and local level, with private industry, and with foreign partners. We must ensure our adversaries do not exploit these new arrangements, which could defeat the very goal of information sharing. In the global war on terrorism, we have entered into partnerships with foreign governments and international organizations whose many views and interests may be different from our own. We must ensure that intelligence sharing is measured against potential risks and sensitive intelligence sources, methods, and operations are safeguarded.

IV. U.S. counterintelligence will safeguard the integrity of intelligence operations and analysis, and defeat foreign intelligence operations.

Intelligence is vital to the formulation and execution of U.S. national security policy and to the Nation's security. Today, the integrity of our intelligence is increasingly challenged, as adversaries seek to deny us insight into their plans and mislead our decision-makers. Therefore,

ensuring the reliability of intelligence becomes a key function of counterintelligence and is a necessary precondition to its very usefulness.

Foreign intelligence services have acquired significant amounts of our classified information, including sensitive U.S. intelligence capabilities. As a result of this knowledge, some countries have become very adept at deceiving and misleading us. These foreign powers attempt to present a false picture of reality through denial and deception operations which increases our uncertainty about their capabilities and intentions. It is the goal of counterintelligence operations and analysis to pierce that false picture, and the threats posed by these adversaries.

An intelligence capability is only as strong as the counterintelligence practices that ensure its integrity. Significant failures in counterintelligence can result in significant failures in positive or foreign intelligence. For example, while a given collection system may yield a wealth of intelligence, it may be useless and misleading if it has been corrupted to show only what an adversary wants us to see. While there are no guarantees that our intelligence collection efforts and our analysis are always accurate, we must establish rigorous procedures to help ensure the integrity of the intelligence that reaches decision-makers. Counterintelligence can supply techniques by which the reliability of a collection system, the *bona fides* of an asset, or the accuracy of an analytic judgment can be validated to ensure its integrity.

V. U.S. counterintelligence will seek to ensure a level economic playing field so that business and industry are not disadvantaged by foreign intelligence operations.

The United States is a nation of commerce and we value the freedom of trade as both a personal liberty and a cornerstone of national wealth. However, if adversaries can exploit the technological accomplishments of industry and gain an unfair advantage, not all trade inures to the Nation's good. While most foreign economic competition is open and lawful, it is not exclusively so. Some business competitors, supported by foreign intelligence services, employ classic intelligence methods in an attempt to gain an advantage over American companies. The outflow of sensitive trade secrets and proprietary information erodes our comparative economic advantage, and undermines national security. Foreign companies that unlawfully

acquire U.S. technology are able to compete unfairly against U.S. firms, which bear heavy research and development costs associated with innovative technology.

As our economy moves toward dependency on the benefits of information technology and networked data systems, our economic well-being and our national security could become valuable to foreign intelligence intrusion and manipulation of our cyber systems. We must ensure that we identify, understand, and counter these threats.

We will seek to identify foreign intelligence operations conducted against U.S. business and industry and we will provide the appropriate threat information to enable them to take such risk mitigation measures as they deem prudent.

VI. The intelligence community will ensure that counterintelligence analytical products are available to the President and his national security team to inform decisions.

To the extent we can observe them, the intelligence activities of foreign powers are a window into their respective interests and plans. Insights into the foreign intelligence activities of others can confirm or shape the prospects for cooperation. Effective counterintelligence analysis can connect the seemingly detached, illuminate hidden relationships, and reveal patterns of activity and behavior previously not observed. In this manner, counterintelligence can supply unique insights into the actions of our adversaries and the actions directed against us, as well as provide opportunities for advancing our own interests.

Counterintelligence represents a philosophic approach that can help bring coherence to many areas of national policy. Effective counterintelligence and security are integral to program efficiency, combat, and operational effectiveness, and foreign policy success. For each national security program, military endeavor, and foreign policy undertaking, there should be consideration for a corresponding counterintelligence plan to help ensure success.

Building a National Counterintelligence System

The counterintelligence capabilities of the United States evolved over time to fit the shape and mission of the disparate institutions in which they are housed. The defined missions of some counterintelligence elements are non-specific, and taken together, these missions do not necessarily provide a response equal to the breadth of the threats arrayed against the United States. Together with their parent national security agencies, these counterintelligence elements must transform to meet the threats of the 21st Century.

Until recently, counterintelligence was an enterprise with no single leadership voice. The counterintelligence community's structure was fragmented and too tactically oriented to provide comprehensive protection to the Nation. The community was not designed to accomplish a strategic mission; rather, the various counterintelligence elements were part of a loose confederation of independent organizations with narrow and differing responsibilities, jurisdictions, and capabilities. Operations tended to focus on individual cases and were conducted with insufficient strategic overview of the potential impact of a synergistic effort.

In the future, each member of the counterintelligence community must be prepared to assume new responsibilities, and join together in a unity of effort, as the *National Counterintelligence Strategy* matures. To be effective, the *National Counterintelligence Strategy* requires that essential processes and features be inculcated into government structures and business models. A national system is needed to integrate, direct, and enhance United States counterintelligence in support of national security decision-making. The features of the National Counterintelligence System include:

National policy leadership and strategic direction. The Director of National Intelligence and the National Counterintelligence Executive, supported by the National Counterintelligence Policy Board, will chart the national counterintelligence mission and will direct and coordinate the resources of the counterintelligence community to accomplish a number of national-level goals including:

- A national program for counterintelligence activities that is strategic, coordinated, and comprehensive in understanding foreign intelligence threats.
- An array of strategic counterintelligence operational and informational options in foreign and defense policy for the President and his national security leadership team.
- A comprehensive assessment and description of foreign intelligence threats and risks to United States national security interests.
- The allocation of counterintelligence community resources prioritized against risk and opportunity.
- Specific counterintelligence policies for attacking foreign intelligence services systematically via strategic counterintelligence operations.

Facilities for cross-agency and cross-disciplinary work. Executing the national counterintelligence mission requires the careful orchestration and integration of many centers of analytic and operational expertise throughout the government. The Director of National Intelligence and the National Counterintelligence Executive will examine the need to establish a national counterintelligence center to integrate threat data, refine collection requirements, and provide a basis for initiating and supporting counterintelligence operations.

Damage assessment process. When national security secrets are lost through espionage or other disclosures, we must assess the loss and impact in order to mitigate damage. In the past, damage assessments received too limited a distribution because of security concerns. We must apply the lessons learned from damage assessments to ensure future vulnerabilities are mitigated. This will require the counterintelligence community take a more centralized approach to these assessments. We will improve the process to support more timely and thorough damage assessments, and ensure the findings are made available to decision-makers with relevant responsibilities.

Resources and performance measurement. The success of any intelligence initiative, sensitive technology development, or national

security program depends in part on effective counterintelligence and security. In the past, counterintelligence support was viewed as an unfunded or underfunded mandate with little consideration of requirements or costs. The planning and budgeting processes should ensure dedicated funding for counterintelligence and security requirements are integrated into sensitive plans and programs. We should seek to ensure the best use of resources is measured against the *National Counterintelligence Strategy* by including performance metrics to chart progress against strategic goals and objectives.

Training and standardization of the counterintelligence cadre. The training and education of collectors, analysts, investigators, and operators in the counterintelligence community has not always been equal to the performance we have demanded of them. The complexity of this subject requires a mastery of many disciplines and skills. The counterintelligence profession needs a set of common standards across many counterintelligence missions. We need to reach across departments and agencies to find centers of training excellence, address deficiencies, and upgrade the availability and uniformity of training.

Intelligence warning process. The disciplines of counterintelligence, with its focus on patterns of and anomalies in activities and behaviors can provide unique insights into foreign intelligence capabilities and intentions. We must ensure the perspectives gained from counterintelligence operations and analysis are incorporated into the intelligence indication and warning process.

Conclusion

At the dawn of the 21st Century, the prospects for freedom, peace and prosperity have never been brighter. Yet we are a Nation at war, and we have suffered grievous attacks on our homeland. The threats we face are grave and diverse, and the intelligence threats that accompany them are equally complex. To respond to these threats, *The National Counterintelligence Strategy of the United States* calls for a proactive response utilizing all of our counterintelligence resources.

The components of this strategic response include:

- Improvements to each of our counterintelligence capabilities to meet the range of foreign intelligence threats: human, technical and cyber.
- All source counterintelligence analysis and strategic planning to drive operations in order to identify, assess, neutralize and exploit foreign intelligence activities before they can do harm to the United States.
- Coordination, integration, and strategic orchestration of the activities of the counterintelligence elements of the government.
- Counterintelligence support to, and involvement by, all national security policy elements of the government.