CHAPTER ELEVEN
COUNTERINTELLIGENCE

Summary & Recommendations

Even as our adversaries—and many of our "friends"—ramp up their intelligence activities against the United States, our counterintelligence efforts remain fractured, myopic, and marginally effective. Our counterintelligence philosophy and practices need dramatic change, starting with centralizing counterintelligence leadership, bringing order to bureaucratic disarray, and taking our counterintelligence fight overseas to adversaries currently safe from scrutiny.

We recommend that:

- The National Counterintelligence Executive (NCIX)—the statutory head of the U.S. counterintelligence community—become the DNI's Mission Manager for counterintelligence, providing strategic direction for the full breadth of counterintelligence activities across the government. In this role, the NCIX should also focus on increasing *technical* counterintelligence efforts across the Intelligence Community;
- The CIA create a new capability dedicated to conducting a full range of counterintelligence activities outside the United States;
- The Department of Defense's Counterintelligence Field Activity assume operational and investigative authority to coordinate and conduct counterintelligence activities throughout the Defense Department; and
- The FBI create a National Security Service that includes the Bureau's Counterintelligence Division, Counterterrorism Division, and the Directorate of Intelligence. A single Executive Assistant Director would lead the service subject to the coordination and budget authorities of the DNI.

INTRODUCTION

Enthusiasm for spying on the United States has not waned since the Cold War. Quite the reverse. The United States is almost certainly one of the top intelligence priorities for practically every government on the planet. Faced with overwhelming American military and economic might, our adversaries increasingly rely on intelligence to gain comparative advantage. A wide range of intelligence activities are used to attack systematically U.S. national security interests worldwide. Yet while our enemies are executing what amounts to a global intelligence war against the United States, we have failed to meet the challenge. U.S. counterintelligence efforts have remained fractured, myopic, and only marginally effective.

Today, we mostly wait for foreign intelligence officers to appear on our doorstep before we even take notice. The lion's share of our counterintelligence resources are expended inside the United States despite the fact that our adversaries target U.S. interests globally. Needless to say, the result is that we are extremely vulnerable outside of our borders.

The losses the United States has sustained within its borders are formidable as well. Spies such as Walker, Ames, Hanssen, and Montes have significantly weakened our intelligence and defense capabilities. Hanssen alone compromised U.S. government secrets whose cost to the nation was in the billions of dollars, not to mention the lives of numerous human sources. Our adversaries have penetrated U.S. intelligence agencies (by recruiting spies) and operations (by running double agents).[1] The theft of some our most sensitive military and technological secrets allows states like China and Russia to reap the benefits of our research and development investments.[2] And while our defense is lacking, our current counterintelligence posture also results in the loss of offensive opportunities to manipulate foreign intelligence activities to our strategic advantage.

Moreover, while stealing our secrets, our adversaries also learn *how* we spy, and how best to counter our efforts in the future, which in turn renders our remaining sources and methods even less effective and more liable to compromise and loss—a cycle of defeat that cannot be indefinitely sustained. As former Director of Central Intelligence Richard Helms once said, "No intelligence service can be more effective than its counterintelligence component for very long."[3]

We believe that U.S. counterintelligence has been plagued by a lack of policy attention and national leadership. We hope this is now coming to a close with the signing of the first national counterintelligence strategy, approved by the President on March 1, 2005. The National Counterintelligence Executive (NCIX)—the statutory head of the U.S. counterintelligence community—has characterized the new offensive counterintelligence strategy as part of the administration's policy of pre-empting threats to the security of the United States.[4]

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.[5] But unlike homeland security, counterintelligence is still largely neglected by policymakers and the Intelligence Community. In fact, counterintelligence has generally *lost* stature since September 11, eclipsed by more immediate counterterrorism needs. While not denigrating it outright, our top policymakers and Intelligence Community management have traditionally paid lip service to counterintelligence. Until, that is, a major spy case breaks. Even then, bureaucratic defensiveness tends to win out. Senior officials have largely addressed counterintelligence issues *ad hoc*, reacting to specific intelligence losses by replacing them with new technologies or collection methods, without addressing the underlying counterintelligence problems.

We offer four recommendations to improve counterintelligence. First, that the NCIX serve as the planner, manager, and supervisor for all United States counterintelligence efforts. Second, that CIA create a new capability dedicated exclusively to attacking intelligence threats outside the United States—a capability our nation currently does not have. Third, that the Department of Defense's Counterintelligence Field Activity be given operational and investigative authority to execute department-wide counterintelligence activities. Fourth, and as discussed more fully in Chapter Ten (Intelligence at Home), that the FBI establish a National Security Service that is fully responsive to the DNI.

Counterintelligence efforts across the Intelligence Community must be better executed in support of the foreign intelligence mission. At the heart of our recommendations is the belief that an integrated and directed U.S. counterintelligence effort will take advantage of intelligence collection opportunities;

protect billions of dollars of defense and intelligence-related investments, sources, and methods; and defend our country against surprise attack.

THE COUNTERINTELLIGENCE CHALLENGE

Spies have always existed, but currently our adversaries—and many of our "friends"—are expanding and intensifying their intelligence activities against U.S. interests worldwide. They target virtually all of our nation's levers of national power—foreign policy and diplomatic strategies, strategic weapon design and capabilities, critical infrastructure components and systems, cutting edge research and technologies,[6] and information and intelligence systems.[7] Our rivals use a range of sophisticated human and technical intelligence techniques, including surveillance, spies, attempts to influence the U.S. media and policymakers, economic espionage, and wholesale technology and trade secret theft. Further, there are indications that foreign intelligence services are clandestinely positioning themselves to attack, exploit, and manipulate critical U.S. information and intelligence systems.

The United States has not sufficiently responded to the scope and scale of the foreign intelligence threat. The number of foreign agents targeting the United States is disturbing—and the majority of them are targeting U.S. interests *outside* the United States. Despite this fact, a very large proportion of U.S. counterintelligence resources are deployed inside the United States[8]—a percentage that has changed very little since the end of the Cold War.

Although we cannot discuss details at this level of classification, suffice it to say that a number of sophisticated intelligence services are aggressively targeting the United States today. These include traditional players such as China and Russia, both of whom deploy official and non-official cover officers to target American interests.[9]

But it is not only major nation states which employ aggressive intelligence services. Terrorist groups like Hizbollah and al-Qa'ida also conduct intelligence operations within the United States. The 9/11 Commission Report, for instance, detailed how the al-Qa'ida hijackers targeted U.S. sites, cased them, and otherwise engaged in classic intelligence activities such as reconnaissance.[10] According to a senior counterintelligence official at CIA, the Agency is only just beginning to understand the intelligence capabilities of terrorist organizations.[11]

Then there are adversaries who attempt to undermine the United States in more subtle ways—through covert influence and perception management efforts. A 1997 Senate investigation found that as many as six individuals with ties to the People's Republic of China sought to channel Chinese money covertly into the 1996 U.S. presidential campaign in order to influence the American political process.[12]

The sum total of these foreign intelligence efforts is striking. During the Cold War, every American national security agency—with the possible exception of the Coast Guard—was penetrated by foreign intelligence services. Moreover, in just the past 20 years CIA, FBI, NSA, DIA, NRO, and the Departments of Defense, State, and Energy have all been penetrated. Secrets stolen include nuclear weapons data, U.S. cryptographic codes and procedures, identification of U.S. intelligence sources and methods (human and technical), and war plans. Indeed, it would be difficult to exaggerate the damage that foreign intelligence penetrations have caused.

THE STATUS QUO

While our rivals have become ever more imaginative and aggressive, our own counterintelligence services remain fractured and reactive. Each U.S. counterintelligence agency pursues its own mission from its own vantage point, rather than working in concert guided by nationally-derived strategies. Our counterintelligence effort has no national focus, no systematic way to coordinate efforts at home and abroad.[13]

Among United States agencies, the FBI dominates counterintelligence within the homeland.[14] Until recently the Bureau focused its resources and operational efforts on foreign spies working out of formal diplomatic establishments—classic official-cover intelligence. The *covert* foreign intelligence presence was largely unaddressed. Today, despite bolstering its counterintelligence resources in all field offices, the FBI still has little capacity to identify, disrupt, or exploit foreign *covert* intelligence activities.[15]

Outside the United States, the CIA has primary responsibility for counterintelligence,[16] a task which, in practice, it defines very narrowly. CIA does not systematically or programmatically undertake the counterintelligence mission of protecting the equities of other U.S. government entities, nor does it mount significant, strategic offensive counterintelligence operations against rival

intelligence services. Its focus is mostly defensive; the CIA's Counterintelligence Center and the counterintelligence elements within the Directorate of Operations aim primarily to protect CIA operations.[17] CIA's current approach to counterintelligence is in contrast to its approach during the Cold War, when CIA case officers routinely targeted Warsaw Pact officials, an effort that led to a considerable number of successful counterespionage investigations.[18]

The Department of Defense, with its component counterintelligence units located within the military services, principally focuses on protecting the armed forces.[19] But no counterintelligence organization has the operational mission for the Department as a whole, leaving large swaths of unprotected areas, including highly sensitive policymaking, technology, and acquisition functions. The current system assigns each of the armed services responsibilities for counterintelligence activities in other agencies that lack their own internal capability. The services, however, do not have the range of capabilities necessary to perform this role. While the Department's Counterintelligence Field Activity (CIFA) has taken steps towards implementing a more comprehensive approach to counterintelligence, CIFA currently does not have adequate authority or resources to take on this Department-wide operational mission.[20]

As if agency-level concerns are not enough, the absence of effective and adequately empowered national counterintelligence leadership makes the situation even worse. The National Counterintelligence Executive (NCIX) is the theoretical "head" of counterintelligence,[21] but NCIX has little control over the scattered elements of U.S. counterintelligence. NCIX has only advisory budget authority, little visibility into individual agencies' counterintelligence operations, and no ability to assign operational responsibility or evaluate performance.[22] The recent intelligence reform act did not alter this situation, but it did take what we believe is a useful step—placing the NCIX in the Office of the DNI.[23]

INSTITUTIONALIZING LEADERSHIP

Recommendation 1

The National Counterintelligence Executive should become the DNI's Mission Manager for counterintelligence, providing strategic direction for the whole range of counterintelligence activities across the government.

Organizational change is not a panacea for counterintelligence, but it is necessary. Today there is no individual or office that can impose Community-wide counterintelligence reform or hold individual agencies accountable for fulfilling national counterintelligence requirements. This should change, and we believe that the obvious candidate for leadership is an empowered NCIX.

The recent intelligence reform legislation situated the NCIX in the Office of the DNI, thereby placing counterintelligence near the Intelligence Community's levers of power. To make this more than window dressing, the NCIX needs all of the DNI's authorities for counterintelligence—particularly authority over the FBI's counterintelligence operations. As the Mission Manager for counterintelligence,[24] the NCIX would build collection plans with prioritized targets and provide strategic direction to operational components. Unlike other Mission Managers, the NCIX would also be responsible for the production of strategic counterintelligence analysis.[25]

To this end, we recommend that the NCIX assume the power and the responsibility to:

- Prepare the National Intelligence Program's counterintelligence budget and approve, oversee, and evaluate how agencies execute that budget;
- Produce national counterintelligence requirements and assign operational responsibilities to agencies for meeting those requirements;
- Evaluate the effectiveness of agencies within the Intelligence Community in meeting national counterintelligence requirements;
- Direct and oversee the integration of counterintelligence tradecraft throughout the Intelligence Community;
- Establish common training and education requirements for counterintelligence officers across the Community, and expand cross-agency training;
- Identify and direct the development and deployment of new and advanced counterintelligence methodologies and technologies;
- Ensure that recommendations emerging from counterintelligence damage assessments are incorporated into agency policies and procedures;
- Deconflict and coordinate operational counterintelligence activities both inside and outside of the United States; and

- Produce *strategic* counterintelligence analysis for policymakers.

These powers would bring the NCIX on par with the other Mission Managers discussed in Chapters Six, Seven, and Eight (Leadership and Management, Collection, and Analysis).[26]

Recommendation 2

The National Counterintelligence Executive should work closely with agencies responsible for protecting U.S. information infrastructure in order to enhance the United States' technical counterintelligence capabilities.

One area we believe is especially critical for the NCIX to address is the absence of a systematic and integrated technical counterintelligence capability. Historically, counterintelligence has been almost exclusively devoted to countering foreign services' human intelligence efforts. At the same time, other organizations like NSA have focused on protecting the U.S. information infrastructure.[27] We therefore recommend that the NCIX devote particular attention to working with agencies that already devote substantial resources to protection of the information infrastructure, looking beyond traditional "counterintelligence" agencies to NSA, other parts of the Department of Defense, the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, and the National Institute of Standards and Technology.

INSIDE THE AGENCIES

Primary responsibility for carrying out counterintelligence activities should remain with CIA, FBI, and the Department of Defense. These agencies, however, need to change the way they fulfill their missions. Under stronger NCIX leadership, they must become the core of the U.S. counterintelligence community—a community with common purpose, focus, and unity of effort.

Recommendation 3

The CIA should create a new capability dedicated to mounting offensive counterintelligence activities abroad.

The CIA should expand its current counterintelligence focus beyond the protection of its own operations to conduct a full range of counterintelligence activities outside the United States. This will require that CIA adopt the mission of protecting the equities of other U.S. government agencies overseas and exploiting opportunities for counterintelligence collection.

We recommend that CIA pursue this mission by establishing a new capability that would—along with the Agency's existing Counterintelligence Center—report to the Associate Deputy Director of Operations for Counterintelligence. This new capability would mount counterintelligence activities outside the United States aimed at recruiting foreign sources and conducting activities to deny, deceive, and exploit foreign intelligence targeting of U.S. interests. In short, the goal would be for the counterintelligence element to track foreign intelligence officers *before* they land on U.S. soil or begin targeting U.S. interests abroad. In doing so, the new capability would complement the Agency's existing defensive operations, and would provide the Intelligence Community with a complete overseas counterintelligence capability. And as with all intelligence activity, the CIA's actions—to the extent they involved U.S. persons—would continue to be subject to the Attorney General's guidelines designed to protect civil liberties.

We must stress that our recommendation is not intended to downplay the importance of continuing to protect CIA operations. These counterintelligence activities must continue, and resources currently allocated to asset validation or other operational counterintelligence capabilities should not be diminished. In this vein, we believe that case officers devoted to the new, offensive activity should be "fenced off" so that they cannot be directed to execute other tasks.

Recommendation 4

The Department of Defense's Counterintelligence Field Activity should have operational and investigative authority to coordinate and conduct counterintelligence activities throughout the Defense Department.

While our intelligence foes strategically target our defense infrastructure, the Department of Defense's counterintelligence response remains hardwired to the 1947 framework in which it was created, with each armed service running

its own counterintelligence component. In 2002, the Defense Department began to address this deficiency by creating the Counterintelligence Field Activity (CIFA), which has the authority to oversee Department of Defense "implementation support to the NCIX," complete counterintelligence program evaluations, conduct operational analysis, provide threat assessments, conduct counterintelligence training, and "oversee Defense-wide CI investigations."[28]

There is, however, one very significant hole in CIFA's authority: it cannot actually carry out counterintelligence investigations and operations on behalf of the Department of Defense.[29] Rather, Defense-wide investigations and operations are left to the responsibility of the individual services—which are, at the same time, also responsible for investigations and operations *within* their own services.[30] Perhaps unsurprisingly, the result of this arrangement is that intra-service investigations are given priority by the services, and no entity views non-service-specific and department-wide investigations as its primary responsibility. What this means is that many Defense Department components (*e.g.*, Combatant Commands, the Defense Agencies, and the Office of the Secretary of Defense) lack effective counterintelligence protection.

We believe this serious shortcoming would be best addressed by giving CIFA the authority and responsibility to provide Department-wide counterintelligence functional support by conducting investigations, operations, collection, and analysis for the Combatant Commands, Defense Agencies, and the Office of the Secretary of Defense, both inside and outside of the United States. The counterintelligence elements within each military service would be left in place to focus on their department's counterintelligence requirements. CIFA would acquire new counterespionage and law enforcement authorities to investigate national security matters and crimes including treason, espionage, foreign intelligence service or terrorist-directed sabotage, economic espionage, and violations of the National Information Infrastructure Protection Act. Specific authorization from the Secretary of Defense and a directive from the DNI can implement this change. And, as with the CIA and service elements, all of CIFA's activities that relate to U.S. persons should be performed in accordance with Attorney General-approved guidelines.

Giving CIFA additional operational authorities will make it a stronger organization better able to execute its current management responsibilities. Today the armed services are not constituted to perform the full range of counterin-

telligence functions that the Department of Defense requires. CIFA will gain greater visibility across the Department and relieve the service counterintelligence components from a responsibility that dilutes resources and effort away from their primary mission—to protect their services from foreign intelligence activities.

Recommendation 5

The FBI should create a National Security Service that includes the Bureau's Counterintelligence Division, Counterterrorism Division, and the Directorate of Intelligence. A single Executive Assistant Director would lead the Service subject to the coordination and budget authorities of the DNI.

With respect to the FBI, we are convinced that a number of significant changes need to take place, largely as part of our recommended creation of a new National Security Service within the Bureau. We address this proposal in detail in Chapter Ten (Intelligence at Home). For current purposes, we merely identify the key reasons why this reform is especially necessary in the counterintelligence field. In our view, bringing the FBI's national security elements under a single Executive Assistant Director responsible to the DNI, and therefore also to the NCIX, would improve the overall effectiveness and strategic direction of FBI counterintelligence and effectively empower analysts to direct collections, investigations, and operations.

CONCLUSION

Since the passage of the National Security Act of 1947, counterintelligence has been treated as a kind of second-class citizen in the intelligence profession. The result is that the subject is pushed to the periphery, our adversaries take advantage of our neglect, and American national security suffers. It is all too easy to forget counterintelligence because, other than periodic spy controversies, there is little public sign that we are doing it poorly. But we are. And our adversaries know it. Our recommended changes—centralizing management and planning, expanding our overseas efforts, and integrating and directing the counterintelligence components of the CIA, Department of Defense, and FBI—are long overdue and will help to stanch the hemorrhaging of our secrets and take the fight to our adversaries.

ENDNOTES

[1] A double agent is a person pretending to work as a spy for one government while actually working as a spy for another government.

[2] Christopher Andrew, *The Sword and Shield: The Mitrokhin Archive* (1999) at pp. 215-220.

[3] Richard Helms, *A Look Over My Shoulder* (2003) at pp. 34-35.

[4] Interview with National Counterintelligence Executive (March 10, 2005).

[5] Interview with National Counterintelligence Executive (Sept. 13, 2004).

[6] FBI, Title classified (Nov. 2004) at pp. 17-18.

[7] Classified intelligence report.

[8] Interview with Office of the National Counterintelligence Executive staff (March 9, 2005).

[9] In our classified report, we include statistics on the estimated Russian and Chinese intelligence presence that we cannot include in our unclassified report.

[10] *Final Report of the National Commission on Terrorist Attacks Upon the United States* (hereinafter "9/11 Commission Report") (2004) at p. 158 & nn. 54, 56; pp. 244-245 (noting al-Qa'ida's casing activities).

[11] Interview with Terrorist Threat Integration Center official (Oct. 6, 2004).

[12] Senate Committee on Homeland Security and Governmental Affairs, *The China Connection: Summary of the Committee's Findings Relating to Efforts of the People's Republic of China to Influence United States Policies and Elections* (1997) at pp. 5-9.

[13] Congress acknowledged this in 2002 when it created the NCIX and, disappointingly, not much has changed. S. Rep. No. 106-279 (2002) at p. 16 (noting inadequate coordination, cooperation, and information-sharing among agencies; a lack of strategic threat analysis; the lack of a national plan to integrate information and analysis; an inadequately prepared workforce with insufficient, diffused resources; and the lack of a national advocate and program for resources, policies, and proactive initiatives).

[14] Executive Order No. 12333 at § 1.14(a).

[15] Interview with FBI Assistant Director for Counterintelligence (Oct. 7, 2005).

[16] Executive Order No. 12333 at § 1.5(e).

[17] Interview with CIA counterintelligence official (Nov. 19, 2004).

[18] *See, e.g.*, Interview with senior official from the Office of the National Counterintelligence Executive (March 9, 2005).

[19] Interview with Department of Defense Counterintelligence and Security official (Oct. 14, 2004); Interview with Department of Defense Counterintelligence Field Activity official (Dec. 14, 2004). "The primary problem is that [Department of Defense] counterintelligence is assigned, under Title X of U.S. law, to the military services as their responsibility, controlled and conducted by them. The military services limit their counterintelligence routinely to support their own missions." Walter Jajko, "The State of Defense Counterintelligence," *Journal of U.S. Intelligence Studies* (Winter/Spring, 2004) at pp. 7-9.

[20] Department of Defense Directive No. 5105.67 (Feb. 19, 2002) at § 6.2.

[21] 50 U.S.C. at § 402b.

[22] Intelligence Authorization Act for Fiscal Year 2003 at §§ 902, 904.

[23] Intelligence Reform and Terrorism Prevention Act of 2004 at § 1011, Pub. L. No. 108-458.

[24] The concept of a Mission Manager is defined more fully in Chapter Six (Leadership and Management), Chapter Seven (Collection), and Chapter Eight (Analysis).

[25] The other exception is the director of the National Counterterrorism Center, the DNI's Mission Manager for Terrorism, who will also be responsible for producing strategic analysis.

[26] We examined other options for improving counterintelligence, but decided that a strengthened NCIX was the best and least disruptive option. Creating a separate national counterintelligence agency, for instance, would involve new legislation, a significant outlay of organizational effort and funding, and disruption of current operations.

[27] *See generally* National Intelligence Council, *Cyber Threats to the United States Infrastructure* (NIE 2004-01D/I) (Feb. 2004).

[28] Department of Defense Directive No. 5105.67 (Feb. 19, 2002) at §§ 6.2.4.1 & 6.2.9.

[29] *Id. at* § 6.2.

[30] Within the Department of Defense, counterintelligence functional support includes investigations, operations, collection, analysis, and functional services. Currently, only the Army, Navy, Air Force, and Marine Corps have authority to do all five activities.