April 2007

School for National Security Executive Education
National Defense University

Counterintelligence and National Strategy

by Michelle K. Van Cleave

Report Documentation Page

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Counterintelligence and National Strategy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,School for National Security Executive Education,Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**44**	

The School for National Security Executive Education (SNSEE) is the newest of the five graduate institutions at the National Defense University (NDU). Its multidisciplinary Master of Arts curriculum in Strategic Security Studies offers concentrations in counterterrorism and international security studies, as well as other fields tailored to sponsoring agencies' professional development requirements. SNSEE programs accommodate full- or part-time Government students in courses, certificates, elective packages, and graduate degrees for which day and evening classes are offered year-round. These include homeland security programs in partnership with the Department of Homeland Security, and Stability, Security, Transition, and Reconstruction in partnership with the Office of the Secretary of Defense and Joint Chiefs of Staff.

SNSEE also executes the NDU International Counterterrorism Fellowship program—the flagship of the Department of Defense (DOD) Regional Defense Combating Terrorism Fellowship Program. One hundred seventy-five counterterrorism specialists from 59 countries have participated in the program since 2003, with 32 students in residence each year from August to June.

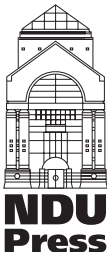
With support and sponsorship from the DOD Counterintelligence Field Activity and the National Counterintelligence Institute, SNSEE is creating an innovative new area of concentration in counterintelligence in order to provide educational opportunities for counterintelligence professionals and to integrate counterintelligence into the broader national security studies curriculum at NDU.

Counterintelligence and National Strategy

Counterintelligence and National Strategy

by Michelle K. Van Cleave

School for National Security Executive Education



National Defense University Press
Washington, D.C.
April 2007

First printing, April 2007

NDU Press publications are sold by the U.S. Government Printing Office. For ordering information, call (202) 512–1800 or write to the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. For GPO publications on-line, access their Web site at: http://www.access.gpo.gov/su_docs/sale.html.

For current publications of the Institute for National Strategic Studies, consult the National Defense University Web site at: http://www.ndu.edu.

Contents

Executive Summary

At the start of the 21st century, there are many more highly capable foreign intelligence services in the world than ever before, and we are only just beginning to understand their modern potential as an extension of state power. The functions that U.S. counterintelligence (CI) performs in the face of these changing intelligence threats have well-established tactical objectives and processes, but their potential as an integral part of American national security strategy is just starting to emerge.

The work of clandestine services, engaged in intelligence collection and other activities, is an arena of international competition in which the advantage does not necessarily go to the rich or powerful. Foreign adversaries may not have a prayer of fielding costly and technologically demanding technical collection suites, but they can organize, train, equip, sustain, and deploy impressive numbers of case officers, agents of influence, saboteurs, and spies, and the United States has become the single most important collection target in the world. Intelligence operations against the United States are now more diffuse, aggressive, technologically sophisticated, and potentially more successful than ever before, especially within America itself, where a rich, free society and an extensive foreign presence provide opportunity and cover for intelligence services and their agents.

Instead of looking at the strategic implications of foreign intelligence operations, we have largely adopted a case-by-case approach to dealing with the threat they represent. By concentrating our CI resources within the United States rather than engaging foreign intelligence services 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.

In 2005, President George W. Bush approved a strategic reorientation of the U.S. CI enterprise to identify, assess, neutralize, and exploit foreign intelligence threats as national security priorities dictate. 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 foreign intelligence services and their ability to work against us, starting with working the target abroad. The tradecraft and operations of counterintelligence are not new. What are new are the 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 offensive.

This strategic mission is a new role for U.S. counterintelligence, which historically has consisted of disparate threat-driven pragmatic activities, each measured on their own terms rather than by their contributions to a larger whole. Without an overarching national CI mission to prioritize threats and articulate goals and objectives, and lacking a national leader to program, conserve, and orchestrate CI activities, the operational elements of the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and military Services have been left to manage their work product to serve their individual ends, creating inherent seams that invite foreign exploitation. Many of the deficiencies that have cost us so dearly have been the result of this systemic failure in the architecture of U.S. counterintelligence.

In the wake of a series of devastating espionage cases, a National Security Council–led review under President Bill Clinton (who signed Presidential Decision Directive 75, "U.S. Counterintelligence Effectiveness—Counterintelligence for the 21st Century") and the U.S. Congress (which passed the Counterintelligence Enhancement Act of 2002) judged that the nature and extent of the foreign intelligence threat required a strategic response and a national mission office to guide its execution. The National Counterintelligence Executive (NCIX) was established by law to ensure the integration and strategic direction of CI community operations and resources. Under the National Counterintelligence Strategy, and as recommended by the Weapons of Mass Destruction (WMD) Commission report issued the same year, the several operational agencies have been asked to assume new responsibilities to execute the strategic CI mission. These include a cadre within the new National Clandestine Service dedicated to executing the strategic CI mission abroad, and a more systemic and strategically driven CI mission at home under the

FBI's newly created National Security Branch. These foundations bring the strategic approach to counterintelligence within reach, but we are not there yet.

Countering foreign intelligence threats to the United States is a compelling national security mission, yet the history of U.S. counterintelligence suggests that fragmentation and lack of strategic coherence will always be the norm—a pattern we tolerate at our peril. If U.S. counterintelligence is to assume the strategic mission that it alone can perform, there are three core imperatives for change.

First, 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 that it has been assigned. In particular, the Director of National Intelligence could 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.

Second, program and budgeting authorities for CI activities remain divided among the departments and agencies, and without the power of a common purse, the mission of integrating and redirecting U.S. counterintelligence to achieve strategic cohesion may well be impossible. Under the old business model, we are getting about the best we could expect out of our CI programs. For the future, avoiding strategic CI failure will require more than simply doing more of the same. While tactical execution must remain with the responsible agencies, coherence should be brought to the CI enterprise through a national program for CI activities that is strategic, coordinated, and comprehensive as to threat.

Finally, the greatest single void at present arises from the compartmentation of information such that 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. While bilateral interaction between the five operational agencies of the FBI, CIA, and the military Services has increased in recent years and especially in the wake of September 11, those contacts taken together do not equal a cohesive, integrated whole. We do not need new bureaucratic structures that take people away from the field, but 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 the disparate operational and analytic activities across the CI community to strategic effect.

Introduction

"Scholarship and the Real World of the Policymaker" sometimes have little in common. In his 1971 article of that name, the journalist and scholar Charles Burton Marshall talked about his undergraduate years as an international relations major in the immediate aftermath of the Great War. In his experience, the coursework did precious little to prepare the student for the world events that were to unfold in the 1930s and 1940s; rather, it centered on legal and institutional readings "full of thoughts fathered by wishes" that "were mostly misleading." In particular, his college studies

> gave no hint of the practices of espionage, the role of intelligence gathering and analysis, or the play of propaganda. States' propensities for leading double lives—having at once forensic and efficient policies, one sort for display, the other to be pursued—were sloughed over.[1]

Over 40 years have passed, and intelligence studies are now a part of most serious international relations departments and are integrated into the curriculum at our nation's war colleges. But the role of counterintelligence remains little known or understood among scholars or practitioners of national security studies and policymaking.[2] In fact, counterintelligence concerns itself with all of the things "sloughed over" in Marshall's critique. The student of today who ignores this dimension of power politics will be even less prepared for the real world than were Marshall's contemporaries. And the national security decisionmaker who neglects the threats and opportunities presented by foreign intelligence activities will be rendering the Nation less prepared for their consequences.

In an effort to help fill this void, this paper offers a twofold contribution to national security studies and advocates some long-overdue changes for U.S. counterintelligence as well. First, it discusses the value of counterintelligence (CI) as a tool of national security and defense strategy, which properly considers the adversary's use of intelligence to achieve advantage and the means necessary to deny that advantage—the mission of CI. Second, it sets forth the elements of a strategic approach to guide U.S. counterintelligence and offers some policy prescriptions to enable the execution of a strategically driven national CI mission.

While these objectives may seem quite ordinary, my experience has been that counterintelligence is little understood by the national security strategist, and strategy is little understood by the CI professional—to the detriment of both pursuits. During my time in office as head of U.S. counterintelligence as well as in this paper, I have endeavored to align the two more closely, both conceptually and in practice. I especially encourage students of defense and strategic studies to pay due attention to the CI discipline. The Nation would benefit from the contributions of scholars and policymakers alike who understand the history, scope, practice, and possibilities of counterintelligence.

Counterintelligence as a Tool of National Security

In the face of changing foreign intelligence threats, the several functions counterintelligence performs have well-established tactical objectives and processes, but their potential as an integral part of U.S. national security strategy is only just beginning to emerge.

When successful, counterintelligence contributes directly to national security by serving both as a shield (guarding against penetrations of our government and informing security and other defensive measures) and a sword (conducting offensive CI operations to shape foreign perceptions and degrade foreign intelligence capabilities) against threats to our nation's security.

Counterintelligence can also contribute indirectly to U.S. policymaking by opening a unique window into the plans, intentions, and capabilities of foreign powers who direct their intelligence operations against the United States or its interests. This window into the "double lives" of states of which Marshall wrote is a less familiar dimension of CI work, one that national security decisionmakers and scholars alike have largely neglected. The positive intelligence that counterintelligence may supply—that is, how and to what ends governments use the precious resources that their intelligence services represent—can help inform the underlying American foreign and defense policy debate, but only if our policy leadership is alert enough to appreciate the value of such insights.

Foreign Intelligence Operations: The New Threat Environment

The proliferation of foreign intelligence capabilities and actors in the post–Cold War world has created a complicated threat environment, with implications for U.S. national security interests at home and abroad that have yet to be fully realized.

Although espionage is often called the world's second oldest profession, the formally constituted external intelligence service is a 20th-century phenomenon.[3] The first American external intelligence service, the Office of Strategic Services (OSS), was born of necessity and with British assistance in World War II. President Harry Truman's decision to disband the OSS after the war was followed by extensive debate over whether the United States needed an external intelligence capability in peacetime, an argument that was finally resolved with the passage of the National Security Act of 1947 and the creation of the Central Intelligence Agency.[4] In rapid succession over the decades since, most of the world's governments have developed some kind of standing external intelligence service.

The overwhelming intelligence threat posed by the former Soviet Union and the Warsaw Pact was the defining concern of U.S. counterintelligence during the Cold War. While the Soviet Union has dissolved, its sophisticated intelligence apparatus remains very much in business. But it is far from alone. At the start of the 21st century, there are more highly capable foreign intelligence services in the world than ever before,

ones that are organized, trained, equipped, and deployed directly against the United States and its interests. And we are only just beginning to understand their modern potential as an extension of state power.

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. Unlike U.S. intelligence, which is highly reliant on national technical means of collection such as signals intelligence (SIGINT) and imagery satellites, most of the world's governments have turned to human collectors to serve as their principal (sometimes exclusive) eyes and ears. At the same time, the information revolution has opened new avenues for intelligence collection through computer network attack and other means, which (especially when enabled by human access agents) can provide potentially high payoff at relatively low cost.

As foreign intelligence activities have grown, the United States has become the foremost collection target in the world. U.S. plans, intentions, and capabilities are the single most valuable information commodity for other governments and nonstate actors, as they chart their own paths for peace, progress, profit, or conflict. One need not necessarily agree with the thesis advanced by Thomas Powers[5] and others that we are in a midst of a long-duration intelligence war to see the value of understanding and protecting against the intelligence operations of enemies, competitors, and even friends.

In recent history, the United States has sustained stunning losses to foreign intelligence services, which used espionage and other means to penetrate almost 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, but thankfully the Cold War ended, as President Ronald Reagan said, without either side firing a shot. Now our nation is at war, engaged in a conflict different in kind and scope than any in our past. Because we are at war, the potential consequences of intelligence and other critical information compromises are more immediate, jeopardizing U.S. operations, deployed forces, and citizenry.

While the immediacy of the threat from Islamic extremist violence is properly in the foreground of U.S. national security concerns, there remain other enduring and persistent dangers from tyrants armed with destructive weaponry and aggressive ambitions, and greater powers whose larger strategic aims we ignore at our peril. With U.S. forces in Afghanistan and Iraq, and American intelligence and special operations teams pursuing al Qaeda networks worldwide, traditional adversaries of the United States, as well as some new ones, see a window of opportunity, and they are seizing it.

Today, most of the world's governments and some 35 suspected terrorist organizations target the United States or its interests for intelligence collection principally through human espionage. Specifically, foreign adversaries use their intelligence capabilities to:

- penetrate, collect, and compromise U.S. national security secrets (information, plans, technology, activities, operations, and so forth) in order to advance their interests and defeat U.S. objectives
- manipulate and distort the picture of reality upon which U.S. policymakers plan and execute national security strategies, technology developments, and economic well-being, including corrupting the intelligence we gather and conducting influence operations aimed at U.S. decisionmakers[6]
- disrupt and counter secret U.S. national security operations (such as covert action, special operations, and other sensitive military and diplomatic activities)
- acquire critical U.S. technologies and other sensitive proprietary information to enhance their military capabilities or to achieve economic advantage.

The use of intelligence operations by weaker powers to achieve advantage is a classic *asymmetric strategy*, a fashionable term but hardly a new concept: "Combatants throughout the ages have continually sought to negate or avoid the strength of the other, while applying one's own strength against another's weakness."[7] For the United States and other democratic countries, our relative "weakness" is the openness of our society and our people. 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 19 hijackers that September morning.

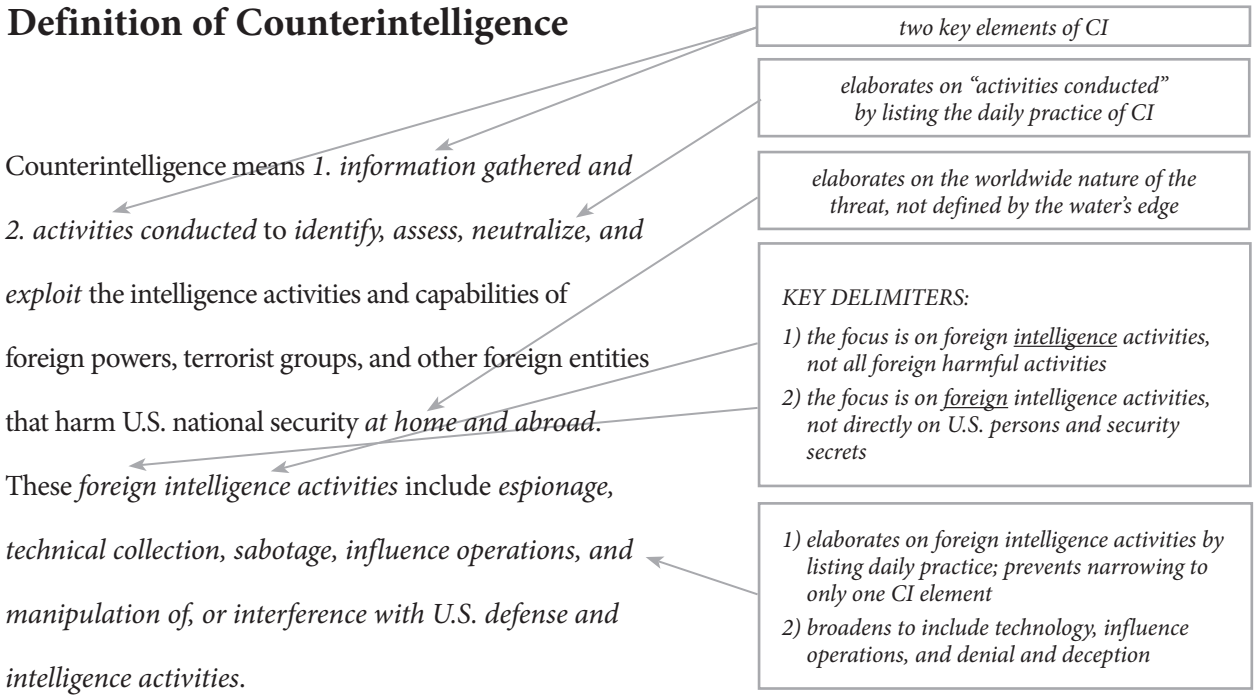
Foreign intelligence operations against the United States are now more diffuse, aggressive, technologically sophisticated, and potentially more successful than ever before. In recent years, increasing intelligence operations within our borders have been facilitated by an extensive foreign presence that 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.

Foreign powers use their intelligence services to seek advantage, and as their objectives diverge, so do the purposes to which their intelligence resources are put. Yale historian Robin Winks reminds us, "As Lenin observed, every intelligence operation has a political object; CI helps to find what that objective is"[8]—and, where appropriate, provide options to defeat it.

The Functions of Counterintelligence

As an integral part of broader U.S. national security policy and strategy, the job of U.S. counterintelligence is to identify, assess, neutralize, and exploit the intelligence activities of foreign powers, terrorist groups, and other entities who seek to do us harm (see figure 1).

Figure 1. Annotated Definition of *Counterintelligence*



Source: Office of the National Counterintelligence Executive.

Identify. The first job of counterintelligence is to identify the foreign intelligence activities directed against the United States and its interests. In its most obvious application, this threat data informs protective security measures (personnel screening, information handling, computer security, physical security) and the dynamic operational security needs of intelligence collection, military activities, and other sensitive national security operations.[9] As with any difficult collection target, the identification of foreign intelligence threats is an iterative process of honing collection requirements, engaging creative collection strategies and techniques, and refining analytic understanding through the demanding standards of intelligence analysis.

But CI analysis also has a specialized and enormously difficult second track: the identification and analysis of "anomalies" that may warn of foreign intelligence successes against us. This is a unique analytic task that takes into account not only what is collected about the foreign intelligence capabilities but also the forensic evidence of their work.

These CI analysts are the ones who zero in on the things that Yogi Berra deemed "too coincidental to be a coincidence." A jumble of many data points—a previously active communications channel gone dark to U.S. SIGINT, a series of human intelligence (HUMINT) reports all conveying the same message, sources compromised in an unknown or suspicious manner, incident reports of intrusions into secure government spaces or information systems—may present a larger picture if they can be collected, lifted above the noise, and correlated with other intelligence about adversary activities and capabilities. Such forensic CI analysis can help discover and connect the seemingly disconnected, discern patterns of activity and behavior heretofore unobserved, and in so doing reveal the hand of foreign intelligence operations.

Visibility into foreign intelligence operations globally can contribute to strategic warning as well.[10] Warning is a highly specialized (and generally not well understood) process, which is both a unique intelligence function and a distinct element of national security decisionmaking. Its essence is the "timely analytic perception and effective communication to policy officials of important changes in the level or character of threats to national security interests that require reevaluation of U.S. readiness to deter or limit damage. The goal is to prevent strategic surprise."[11] As described by the House Permanent Select Committee on Intelligence:

> Warning occupies a central and a unique role in U.S. national security planning as well as in the intelligence community. A timely warning provides the opportunity for policy makers to engage early in threat management, thereby possibly deterring or defusing a crisis and reducing the political as well as the economic cost to the nation. Even late in the crisis, accurate warning can assist the decision maker in effectively utilizing national security resources, thus favorably altering the outcome.[12]

As part of a warning template, the activities of foreign intelligence services may number among the most useful early indicators of changes in threat conditions. Intelligence activities are classic precursors to attack. When the warning community was concerned about an attack on the North Atlantic Treaty Organization (NATO) through the Fulda Gap, U.S. intelligence kept watch for missile and aircraft readiness stages and forward movements of armor and personnel. Warning of attack in the current threat environment is more subtle, but intelligence preparation is a necessary precondition even for terrorist attacks. As the Defense Science Board pointed out in October 2001, "No observation is more important in countering terrorism than to understand that would-be perpetrators, to succeed, must participate in the gathering and application of intelligence."[13]

Similarly, the presence of foreign intelligence personnel or operations in a third country may reflect an expectation of a new collection opportunity or, when correlated with other events or processes, present a pattern indicating a new development such as preparation for a covert initiative. For example, a noticeable increase in the Chinese intelligence presence in Latin America might be an anomaly that keys U.S. collection to other indicators of Chinese interest or transactions, which in turn might give warning analysts some insight into prospective significant geopolitical changes.

Timeliness and reliability are the keys to effective warning, which means that the sooner U.S. intelligence gets wind of changes to come, the greater the opportunity it has to validate the indicators of change and issue timely warning. The commitment of foreign intelligence resources reflects choices that must be made early in the decision cycle as their governments weigh threat and opportunity and prepare to act.

Given the substantial costs (funding, risks, and opportunity costs) involved in the allocation and targeting of scarce intelligence resources, their presence can serve as early precursors of emerging threats. Observed changes in foreign intelligence activities may also serve as red flags to help hone collection on related indicators of threat to inform warning decisions better.

For the decisionmaker, timely warning intelligence needs to be evaluated in the context of national security objectives, the political/military environment in which the threat is developing, and the range of options available to influence the adversary or mitigate exposure. The purpose of warning is not merely to trigger the equivalent of a call to "*Take cover!*" but also to enable actions to manage the threat, including actions that might dissuade the adversary from initiating conflict and limiting damage. Only with the long leadtime of strategic warning can policymakers engage the full range of diplomatic, economic, and other pressures to shape a favorable outcome. A greater awareness of foreign intelligence activities may help lengthen that leadtime, as well as suggest additional options to influence events, as discussed below.

Assess. Analysis of the intelligence activities of adversaries or allies, competitors or partners, may open a window into their respective interests, purposes, and plans. For instance, our insights into the foreign intelligence activities of the other main centers of global power may confirm or otherwise shape prospects for cooperative action.

U.S. policy toward Russia is a case in point. Many of the Cold War activities of the Soviet-era *Komitet Gosudarstvennoi Bezopastnosti* (the Committee for State Security, or KGB) are recounted in the book *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*.[14] Drawing on unprecedented access to over 25,000 pages of KGB files, the authors document the breadth and audacity of the former Soviet intelligence attack on the United States—including notably its extensive active measures and disinformation campaign, which would appear to have confirmed the most conspiracy-minded suspicions of the anticommunist American right wing. As one observer points out, the real importance of the book is "the sheer weight of accumulated detail which reveals a madly compulsive Soviet over-reliance on clandestine means for conducting its foreign policy, maintaining security and ideological control at home, and acquiring the technological infrastructure of a modern state."[15] The extent to which Russia continues this 70-year tradition of aggressive clandestine operations in the United States and elsewhere should be of no small interest to national security decisionmakers as they fashion U.S. policy toward the government of (former KGB/Federal Security Bureau head) President Vladimir Putin.

Intelligence services are a tool of state power. Their uses are many, as are their corresponding strengths and weaknesses. Within the disciplines of international relations or comparative politics, there is room for far more study of both the diversity of intelligence services as government institutions and of intelligence operations as an extension of state action. In practice, CI tasks must be prioritized by a sophisticated assessment of threats, which proceeds from an understanding of how intelligence capabilities are used to advance foreign objectives.

Consider the case of China's intelligence activities, which increasingly rival those of Russia as a U.S. counterintelligence concern. We know that the most likely way the United States and China could come to military conflict is over Taiwan and that such a conflict is likely to involve naval engagements. There are specific dimensions to those engagements that would shape Chinese intelligence collection objectives against U.S. targets, within Taiwan, and elsewhere in the region (and globally as well). Scenario-driven logic trees of this kind can yield a taxonomy for prioritizing CI analytic efforts and drive collection to support that analysis.

Assessments of foreign intelligence capabilities can help inform policy deliberations and frame options for actions, supplying answers to such questions as:

- 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?

- 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 Hugo Chavez's government?
- What efforts are under way 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?[16]

The foreign intelligence activities of adversaries and friends are an important factor to consider as part of sound national security policymaking. Counterintelligence can supply specialized insights, provided that the allocation of CI collection and analytic resources are prioritized to support policy needs. For example, Israeli intelligence activities worldwide are a matter of no small CI concern,[17] but they are far down on the U.S. national security priority list relative to perhaps less capable but far more worrisome intelligence activities of hostile states. The judgment of whether CI resource allocations are providing the greatest return on investment may differ depending on whether the measure of effectiveness is national security policy relevance or operational insight. Analytic support to CI operations is a vital CI function. Foreign intelligence threat assessments that are driven by national security policy are a strategic CI mission.

Neutralize. Counterintelligence has a positive intelligence role to identify threats and assess foreign intelligence capability, but that is only the beginning. The most distinguishing feature of counterintelligence is that it is an operational function. As defined in law by the National Security Act of 1947, *counterintelligence* is "information gathered *and activities conducted* [emphasis added] 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."

"For the intelligence-minded man, to know about the opposition and his installations is the whole goal; for counterintelligence, knowing is only the beginning of the road—something has to be done about the information."[18] The emphasis on *doing* extends beyond the Intelligence Community to include elements of law enforcement. When a spy is arrested, or a "diplomat" caught *in pari delicto* and expelled, or an asset discredited as working for the other side, the CI elements that neutralized the foreign intelligence operation have done their specific job.

Stepping up to the strategic level, the neutralization of foreign intelligence threats is an essential part of protecting national security secrets. Sound security measures such as locks, guards and gates, background investigations and polygraphs, computer firewalls and document controls, are unquestionably vital, but they can only carry protection so far; there will always be a purposeful adversary looking for ways to get at what it wants. Counterintelligence goes after the adversary.

Campaigns to neutralize enemy intelligence capabilities have long been an essential part of war planning. They also have a place in national security strategy in times of peace. One of the best examples of strategic CI operations was the work that began in the early 1980s to stop the Soviets' illicit acquisition of advanced technologies. The détente policies of the Nixon administration had opened the floodgates to Soviet intelligence in their clandestine efforts to obtain scientific knowledge and technologies from the West:

> This effort was suspected by a few U.S. Government officials but not documented until 1981, when French intelligence obtained the services of Colonel Vladimir I. Vetrov, codenamed "Farewell," who photographed and supplied 4,000 KGB documents on the program. In summer 1981, President François Mitterrand told President Reagan of the source, and, when the material was supplied, it led to a potent counterintelligence response by CIA and the NATO intelligence services.[19]

The Farewell dossier provided detailed information on Soviet technology acquisition efforts, including how the collection program was run under Line X (the KGB division in charge of gathering science and technology information) and exactly what they were after. It set off a far-reaching technology control

effort, including export control enforcement actions and effective international cooperation in interdicting unlawful transfers. And U.S. intelligence implemented a new set of requirements to develop follow-on sources to expose true end users and other valuable insights into Soviet technology acquisition activities. The ensuing CI operations to disrupt Soviet technology collection were broad and thorough. Within the United States, and jointly with NATO governments in Western Europe, some 200 Soviet intelligence officers and their sources were compromised and expelled, effectively putting Line X out of business.[20]

Importantly, this strategic CI campaign was of a piece with the larger U.S. strategy toward the former Soviet Union under the Reagan administration. Embodied in National Security Decision Directive 75, the central objective was to "contain and over time reverse Soviet expansionism by competing effectively on a sustained basis with the Soviet Union in all international arenas."[21] The U.S. defense buildup of the 1980s was the centerpiece of this strategy. When Farewell walked through the door, the United States was just beginning a military modernization effort that would rest the Nation's defenses on capturing and sustaining qualitative superiority. Research and development (R&D) efforts supporting the Strategic Defense Initiative, new composite materials enabling stealth capabilities, and breakthroughs in supercomputing and other extraordinary information technologies, among many other marvels of engineering and design, were all at stake.

Farewell gave U.S. counterintelligence the keys to neutralize the KGB's campaign to piggyback on U.S. technology investments. But that was not all.

Exploit. The opportunity was tantalizing. "With the Farewell reporting," as the late Gus Weiss told the story, "CIA had the Line X shopping list for still-needed technology, and with the list American intelligence might be able to control for its purposes at least part of Line X's collection, that is, turn the tables on the KGB and conduct economic warfare of our own." Weiss continued:

> I met with Director of Central Intelligence William Casey on an afternoon in January 1982. I proposed using the Farewell material to feed or play back the products sought by Line X, but these would come from our own sources and would have been "'improved," that is, designed so that on arrival in the Soviet Union they would appear genuine but would later fail. U.S. intelligence would match Line X requirements supplied through Vetrov with our version of those items, ones that would hardly meet the expectations of that vast Soviet apparatus deployed to collect them.
>
> If some double agent told the KGB the Americans were alert to Line X and were interfering with their collection by subverting, if not sabotaging, the effort, I believed the United States still could not lose. The Soviets, being a suspicious lot, would be likely to question and reject everything Line X collected. If so, this would be a rarity in the world of espionage, an operation that would succeed even if compromised. Casey liked the proposal.
>
> As was later reported in *Aviation Week & Space Technology*, CIA and the Defense Department, in partnership with the FBI, set up a program to do just what we had discussed: modified products were devised and "made available" to Line X collection channels.[22]

There has been no official confirmation of the existence of the program Weiss describes. Indeed, if Line X collection was being shut down through a vast expulsion effort, it would be tricky to salt the collection channels simultaneously in the manner Weiss suggests. However, the concept of using the adversary's own intelligence operations against them is a stellar example of creative offensive CI.

Golden opportunities of the kind Farewell provided do not come knocking every day. But the national CI enterprise needs to be constituted to seek out high-value insights into foreign intelligence activities, recognize gold when it appears (and fool's gold for what it is), and be creative and agile and competent enough to seize the moment.

The world of offensive counterintelligence is most familiar in its supporting role to military operations.[23] The finest historic example is the Allied landing at Normandy. The D-Day landing was a huge risk that succeeded because of masterful planning, including the most sweeping deception in military history. The Allies could not hope to hide the fact that they intended a cross-channel invasion, but through the use of elaborate decoys and ruses, misleading communications, finely orchestrated double agent operations,[24] and a host of other inventive measures, they led the Germans to believe the landing site would be at Pas de Calais. The surprise was total.[25]

For deception to be successful, according to World War II historian F.H. Hinsley, "two things are imperative: First, the enemy must be kept totally in the dark about what you don't want him to know, and second, you must know everything he is thinking all the time, especially when he's confronted with what you want him to believe." In any deception campaign, the feedback loop is all important. Hinsley continues:

> We were able to locate, early on, the entire German espionage network in Britain, eliminate parts of it and use others to feed Hitler disinformation. We were also able to learn Hitler's thinking about where and when the invasion would eventually come, play to his prejudices and hunches, and learn when and whether he took our bait. We were reading his mind all the time.[26]

Offensive CI seeks to influence the adversary's decisionmakers by manipulating the intelligence product that informs their decisions, "luring your opponent into doing voluntarily and by choice what you want him to do."[27] This was the role counterintelligence played in Operation *Overlord*, luring the Germans to mass their forces in the wrong place.

The same principle pertains to the role counterintelligence can play in peacetime. Successful counterintelligence operations can provide the means for influencing decisions or behaviors that may spell the difference between favorable or unfavorable outcomes in world events. The key to success in counterintelligence, like everything else, is playing to your strengths—or to the adversary's vulnerabilities.

Foreign emphasis on human collectors over other means of collection is the single most distinctive asymmetry in modern intelligence structures, and it has profound implications for U.S. counterintelligence. The U.S. Intelligence Community had its origins in Pearl Harbor and the imperative to guard against strategic surprise. Our money and genius went into the development and fielding of an early warning capability to watch for missile launches, and standoff capabilities to pierce the Iron Curtain and to learn all we could about the unparalleled Soviet threat. We tend to place greater trust in what we collect through sophisticated technical means than through human channels with their many idiosyncrasies and limitations. In this history, U.S. intelligence is distinctive.

In sharp contrast, HUMINT is necessarily the bread and butter of our adversaries and friends.[28] An early Soviet defector contrasted what he saw as the Western approach to intelligence collection of monitoring the world scene for voluminous bits of open data with the Soviet reliance on the work of spies: "The difference is not just a theoretical one; in practice it affects every phase of intelligence activity, from operational strategy and choice of strategy to evaluation of the reliability of information procured and its importance to policy makers."[29] It also affects relative strengths—and vulnerabilities.

The work of clandestine services, engaged in intelligence collection and other activities, is an arena of international competition in which 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 (the U.S. Government has worked 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—which they do, in numbers commensurate with their value.

Yet there is wisdom in the notion that every strength can become a liability. If HUMINT is the eyes and ears of foreign leaders, purposefully shaping the reporting they receive through HUMINT channels can be a formidable influence on their actions. And the foreign intelligence service becomes an even more attractive target for penetration.

The ultimate goal of offensive CI

> is to penetrate the opposition's own secret operations apparatus: to become, obviously without the opposition's knowledge, an integral and functioning part of their calculations and operations. . . . [A successful CI penetration] puts you at the very heart of his actions and intentions towards you. . . . Most importantly, you are in a position to control his actions, since you can, by tailoring intelligence for him to your purposes, by influencing his evaluation, mislead him as to his decisions and consequent actions.[30]

To be sure, this describes the ideal CI operation; but even short of such perfection, by exploiting insights into foreign intelligence activities, counterintelligence can provide new avenues to degrade emerging threats and help turn events to U.S. advantage.

The tradecraft and operations of counterintelligence are not new. What is new are the possibilities of forging closer ties to national strategy by integrating CI insights into national security planning; prioritizing CI collection and operations in line with national security priorities; and, at the strategic level, going on the offense.

National Security Strategy under President Bush

The National Security Strategy of the United States of America, issued by President Bush in 2002 and updated in 2006, proceeds from a fundamental objective: "to create a balance of power that favors freedom." That document is very much an offensive strategy, including in particular its emphasis on preemption and preventive measures. This offensive aspect has made the President's strategy both distinctive and controversial.

John Lewis Gaddis, in his monograph *Surprise, Security, and the American Experience*, argues that the Bush doctrine is far more serious and sophisticated than its critics acknowledge—and also less novel. He points out that the United States has suffered three surprise attacks in its history, each of which called forth a new grand strategy: the British burning of Washington, DC, in 1814; the Japanese attack at Pearl Harbor in 1941; and the attacks of September 11, 2001. As Gaddis writes, "Americans have generally responded to threats—and particularly surprise attacks—by taking the offensive, by becoming more conspicuous, by confronting, neutralizing, and if possible overwhelming, the sources of danger rather than fleeing from them."[31]

Accordingly, in the wake of the British attack, new Secretary of State John Quincy Adams developed America's first confrontational grand strategy, which was twofold: to achieve security through territorial expansion in order to preempt the power vacuum on the continent, and to adopt a policy of unilateralism and thus avoiding entangling alliances. The second American grand strategy arose under Franklin Roosevelt, who sought to secure the United States by securing the world, guaranteeing free markets and self-determination for all people. Strong states, acting through the United Nations Security Council, would secure the peace. This grand strategy saw us through the Cold War.

Now we have a new enemy and new threats, which require means different from those employed during World War II and the Cold War. In response, Gaddis argues, the Bush doctrine is not so much a departure from American history as a return to the preemption and unilateral action of the 19th century. Today's new element is the need to walk a fine line to hold on to the consent of key states, which is not an easy task. The many difficult issues associated with counterterrorist operations, including extraordinary renditions, long-term imprisonment of detainees, and other intelligence and operational exigencies, have been grist for anti-American propaganda mills and diplomatic confrontations.

Personal politics notwithstanding, all responsible citizens of the United States agree that we cannot wait until the threat reaches our shores to act. In the past, terrorists were subject to manhunts, apprehension, and rendition for trial. Today, the strategic objective is to stop them before they can strike. The same imperative should apply to the intelligence operations of our adversaries.

The Best Defense is a Good Offense

The record of U.S. counterintelligence, especially counterespionage, shows that most CI has been based on tolerating some level of loss—extremely grave loss in the case of some long-serving, well-placed spies—that, once discovered, triggers intensive investigations, prosecutions, and countermeasures to repair and limit damage. This ability to react quickly and effectively will always be a vital core of counterintelligence. But a strategy predicated on acceptable loss was always a questionable approach to countering hostile intelligence activities, which could have failed catastrophically had the United States found itself at war with the Soviet Union. It is now intolerable in the face of a global war and the steady growth of intelligence operations directed against the United States and its interests.

Other states, and certainly all of our adversaries, seek to use their intelligence services as a strategic make-weight. Not surprisingly, U.S. counterintelligence is identifying collection activities targeted against all the essential elements of our national defenses and the supporting structures that maintain the Nation's technological advantage at home and abroad. From the standpoint of foreign intelligence interest, there are many potentially valuable targets outside of our borders, such as American Government personnel and the far-reaching activities of critical U.S. commerce and industry. But the real intelligence treasure trove for foreign powers is in the United States.

The institutions and people responsible for the formulation and implementation of American plans, intentions, and capabilities—the central targets of foreign intelligence collection and influence—are principally within the borders of the United States. Intelligence production and weapons design, the secrets of our nuclear labs, and the strategic advantage afforded the Nation's security by R&D at American companies such as Bell Labs or Boeing or Dupont are all within our borders, as are thousands of facilities engaged in classified national security work and hundreds of thousands of workers who hold security clearances. If these structures and personnel have become the principal target of foreign intelligence operations, an effective CI capability is our first and last means of defense to protect them.

Today, for example, notwithstanding our relatively friendly relationship at the political level, the Russian intelligence and security services remain our most capable adversaries, both abroad as well as in the United States, where they continue to operate as though the Cold War had not ended. With the explosion of the volume of Russian and other tourists, immigrants, official visitors, and business operations in this country, the opportunities for clandestine operations have increased proportionately.

The CI problem is not one of sheer numbers, though by any measure there are more foreign intelligence operatives in the United States than we have personnel to address them.[32] The larger and more compelling issue is the scope of their activities.

Historically, embassies and other diplomatic establishments within the United States have served as the hub for foreign intelligence activities because of the operational security they afford. Not surprisingly, the 20,000-strong diplomatic community has commanded the lion's share of U.S. counterintelligence attention. Our CI resources, especially those of the FBI, have been scoped against this threat population and its geographic concentrations in Washington and New York, and consular offices in such cities as San Francisco, Chicago, Atlanta, and Houston.

Now, however, foreign powers increasingly are running intelligence operations with unprecedented independence from the former safe havens of their diplomatic establishments. The number of formal and informal ports of entry to the country, the ease with which people can travel internally, and the relatively benign U.S. operational environment are tailor-made for embedded clandestine collection activities. Thousands of foreign-owned commercial establishments within the country, the routine interactions of trade and transnational business and finance, and the exchange of hundreds of thousands of students and academicians all potentially extend the reach of foreign intelligence into the core structures of the Nation's security.

Instead of looking at the strategic implications of these foreign intelligence operations, we have for the most part adopted a case-by-case approach to dealing with the threat they represent. Domestically, our CI effort has been concentrated on counterespionage investigations: violations of criminal statutes against espionage and related offenses (such as failure to register as a foreign agent, mishandling of classified information, and certain violations of export control laws). 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.[33]

As a result, I fear we have been somewhat oblivious to the effects of foreign intelligence operations within the United States except when they find expression in espionage cases. While the FBI—by far, America's premier CI agency—is assigned responsibility for countering all foreign intelligence operations in the United States, it lacks the manpower, the resources, the training, and probably the public support to venture into the complex grounds of analyzing the vast foreign presence in the country to identify the intelligence operations embedded therein.[34] No other department or agency is assigned this mission, sees it

as their job, or has the authority to carry it out. As a result, our understanding of the foreign presence and intelligence operations within the United States is unacceptably poor.

Yet three-quarters of the American CI budget since World War II has been devoted to activities within the United States carried out by the FBI. In addition, most of the remainder allocated to the CIA, Defense Department, and to small pockets elsewhere in the government has gone to programs and personnel based wholly or in part within U.S. borders. As a national priority, funding for counterintelligence is pitifully low relative to the penalty foreign intelligence successes can exact. But more money is not the cure, so long as the resulting business model of U.S. counterintelligence remains optimized for a defensive posture of working individual cases at home, rather than working the foreign intelligence service as a strategic target globally.

In the past, America's default CI strategy has been to wait to engage the adversary in our own backyard, rather than in his. Again by default, we have placed ourselves at a twofold disadvantage. By concentrating our CI resources within the United States, and waiting for the foreign intelligence threat to come to U.S. territory, we have ceded the advantage to the adversary. Foreign powers have seized the initiative and have moved their operations to favorable terrain: U.S. soil. Our domestic institutions are not constituted to work against foreign intelligence cadre embedded within American society; indeed, we have laws and constitutional values that militate against government intrusion (by intelligence entities or law enforcement agencies) into private life—an operating advantage that foreign services readily exploit.

The strategic implications are clear. We have been approaching the problem from the wrong end. Rather than waiting until the foreign intelligence threat is at our doorstep, U.S. counterintelligence needs to go on the offense, to exploit where we can and interdict where we must, with the purpose of degrading the foreign intelligence service and its ability to work against us.

Assigning a strategic, proactive mission to U.S. counterintelligence represents a sharp departure from past practices. In my view, this expansion and strategic reorientation of the U.S. CI enterprise are long overdue. No longer can we afford to rest on our ability to tolerate some level of loss before taking action. No longer should we cede the initiative to foreign intelligence services working on U.S. soil to penetrate our government. The age-old wisdom that the best defense is a good offense is also true for counterintelligence.

Executing an offensive CI strategy begins with working the target abroad. As directed by national security policy priorities, the considerable resources of the members of the U.S. Intelligence Community that have global reach need to be directed to help identify and then disrupt or exploit the intelligence activities of foreign powers, wherever they are directed against U.S. interests worldwide. Conceptually, this undertaking consists of two parts: first, a global CI assessment of foreign intelligence presence, capabilities, and activities, and second, a CI "doctrine"—the fundamental principles that guide military or other operations in support of national objectives—for attacking foreign intelligence services systematically via strategic CI operations.

At home, the proactive CI mission calls for a coordinated, community-wide effort of aggressive operational activity and analysis to obtain the intelligence necessary to neutralize the inevitable penetrations of our government. To do this, the operational and analytic focus of U.S. counterintelligence must transform from a case-driven approach to a strategic assessment of adversary presence, capabilities, and intentions, which in turn drives operations. This will also require looking beyond the customary targets of known intelligence officers to the larger population of diverse foreign visitors and others serving foreign intelligence purposes, who find our free and open society a rich playing field for the illicit collection of national security secrets and other valuable information that confer advantage.

We need to find appropriate ways, consistent with all the protections of our Constitution, to discern foreign operations within the United States. What can be done to fill the enormous gaps in our knowledge? With some 500 million border crossings annually, this is a nearly overwhelming problem for U.S. counterintelligence, as it is for our Nation's counterterrorism efforts. Yet despite these odds, the painstaking network analysis of al Qaeda cells is paying off, which may suggest an approach for CI analysis as well. Similarly, the Defense Department has hard-won experience with locating elusive targets against a vast background of noise; there may be an analogous methodology that can provide clues on how to find hidden foreign intelligence operations in the United States.

Most of today's CI professionals came to the profession through specific training in intelligence or in investigations and law enforcement. Much of their work involves careful watchdog activities that zero in on indicators of internal wrongdoing, security glitches, suspicious transactions, or other anomalies. In this respect, while individual investigators and intelligence officers may perform their job with great personal initiative, counterintelligence as a national enterprise is largely reactive and tactical. We need to take that personal initiative and turn it into national initiative.

The proactive approach to counterintelligence requires a generous dose of creativity to turn threat into opportunity. We do not want to sit back and discover, years after the fact, that while we have investigated every reported security breach, spies have stolen our secrets or cyber thieves have exploited our networks. Instead, U.S. counterintelligence needs to think offensively: how does the foreign intelligence service operate? What are its vulnerabilities? How can they be exploited? What are the indicators that might give us warning of intelligence operations against us? Are there tripwires we can design to give us an edge? Are there CI avenues available to influence foreign decisionmaking to help achieve larger U.S. national security objectives? There is no question that our Nation's talented CI professionals can do this job, provided their leadership sets the right course. Clearly, U.S. counterintelligence needs a new strategy, and now it has one.

The 2005 National Counterintelligence Strategy

Each of 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—has an embedded counterintelligence imperative. Specifically, terrorists, tyrants, foreign adversaries, and even economic competitors engage in a range of intelligence activities directed against us in order to advance their interests and defeat U.S. objectives.

Too often, these foreign intelligence activities against the United States are successful. Collectively, they present strategic threats to the Nation's security and prosperity. The United States requires a national, systematic perspective and coherent policies to counter them. Key to success is a strategic counterintelligence response.

We now have, for the first time, a single document that sets forth the President's vision for U.S. counterintelligence and its mission in support of America's national security. President Bush approved the National Counterintelligence Strategy on March 1, 2005, while Congress was still debating the creation of the Office of the Director of National Intelligence. The new strategy is the product of contributions from across the leadership of the CI community, and in its final form is the result of careful White House deliberation and review. It is the first document issued by any administration that directs the full scope of the Nation's efforts to counter the global foreign intelligence threats against the United States.[35]

The National Counterintelligence Strategy, which is unclassified, is based on a classified threat assessment that lays out the ways in which foreign intelligence services are stealing U.S. national security secrets to support their military or terrorist objectives, to undercut America's foreign policy or commerce, or to exploit what they learn of U.S. intelligence capabilities to hide their actions or mislead us.[36] The strategic purpose of counterintelligence is to identify these threats and stop them.

Modeled after the President's National Security Strategy, the 2005 National Counterintelligence Strategy has seven pillars that define the objectives for U.S. CI: counter terrorist operations, seize advantage, protect critical defense technology, defeat foreign denial and deception, level the economic playing field, inform national security decisionmaking, and build a national CI system.

Counter Terrorist Operations. In many parts of the world, including in the United States, al Qaeda and other terrorist organizations employ classic intelligence methods to gather information, recruit sources, and direct human assets. They are also capable of engaging in sophisticated deceptive practices, not unlike traditional foreign powers, to mislead U.S. decisionmakers. Beyond this, terrorist groups draw strength from state sponsors, which means that the intelligence services of those regimes can be key links in the global terrorist support network.

The National Counterintelligence Strategy directs the national security leadership to ensure that the war on terror is armor-plated with an effective CI strategy to identify and exploit offensive opportunities against terrorist networks and to provide CI support to force protection and operations security in the field. We need to institutionalize the linkages between counterintelligence and the analytic and operational entities supporting the global war on terrorism—a critical element that the September 11 Commission overlooked. Behind these straightforward objectives lie many intensive tasks, such as bringing analytic insight into the intelligence operations of terrorist groups and their sponsors, providing CI support to sensitive U.S. operations, and developing a CI mindset to backstop the geopolitical imperatives of this global war.

As an integral part of the U.S. campaign against radical Islamic terrorist groups, it is the job of counterintelligence to develop and execute integrated strategic operations against the intelligence activities of terrorist groups and their state sponsors. In theory, terrorist groups have positive intelligence objectives and need to protect their operations. What does that intelligence footprint look like, and how amenable are these operations to CI remedies or solutions?

The intelligence activities of state sponsors of terrorism are a related category of CI interest. As part of a larger effort to document the range and details of state actor support to terrorist organizations or activities, counterintelligence needs a collection plan for foreign intelligence support to terrorists that can enable CI operations to degrade their success. Obvious collection requirements include such details as knowing the names of foreign intelligence personnel and how and from whom they receive their tasking. The CI discipline affords both the strategic analytic perspective and the operational tradecraft needed to identify and exploit offensive opportunities against terrorist networks and the intelligence operations of their state sponsors.

The war on terror has led to an expanding number of cooperative intelligence relationships, some of which draw on longstanding liaison histories, and others of which are very high risk. The United States has established these intelligence relationships because we have a genuine purpose to go after terrorist groups. Other states may have different (or supplementary) motivations for cooperative intelligence work. Across the board, counterintelligence needs to assess how foreign intelligence services are exploiting their relationship with the U.S. counterterrorism effort for their own purposes.

Intelligence liaison relationships are one among myriad U.S. counterterrorism activities that require a CI plan. The many elements of the U.S. national security community engaged in counterterrorist work, from the dedicated analytic and planning elements of the Intelligence Community to the U.S. forces deployed in Iraq and Afghanistan to Special Operations teams in many parts of the world, are targets of foreign intelligence and al Qaeda interest.

There are also troubling questions surrounding the true extent of initiatives by terrorist organizations or their agents to penetrate supporting elements of the U.S. Government. Our generation's struggle against the extremist teachings of radical Islam is a war for hearts and minds and a breeding ground for ideological spies.[37] Public reports suggest that some 40 terrorists had been caught trying to infiltrate U.S. intelligence agencies as of 2005,[38] leading to no small concern over how many may have escaped detection. Each of these endeavors is a proper, and compelling, subject for U.S. counterintelligence.

Seize Advantage. In line with broader national security objectives, the National Counterintelligence Strategy directs that U.S. counterintelligence shift emphasis from a posture of reacting to foreign intelligence threats to a proactive strategy of seizing advantage.

The need for this capability was driven home in our experience with the war against Iraq. In the leadup to Operation *Iraqi Freedom*, an interagency CI strategic planning team came together to develop a common operating picture of Iraqi intelligence operations worldwide. In response to command authority direction, the team was chartered to render Iraqi intelligence ineffective. While this effort resulted in some important successes, the CI community learned its lessons the hard way:

- Strategic operational planning to degrade foreign intelligence capabilities has long leadtimes. Beginning at D minus 6 months—as was the case with Iraq—is too little, too late. Even though coalition forces had technically been at war with Iraq for 10 years, flying daily combat missions, the CI community could identify and contain an unacceptably low percentage of Iraqi intelligence personnel.

- U.S. counterintelligence was not (and is not) postured globally to disrupt a foreign intelligence service. U.S. capabilities are not integrated to operate jointly. There is a basic lack of central orchestration or of a standard approach to targeting. Interagency information-sharing is poor, and infrastructure support is even worse.

The interagency, proactive approach adopted in the leadup to Iraq is the right way to go, but it will not work if it is ad hoc. Resources need to be prepositioned, and real CI operations plans built in advance, including command over non-CI resources (especially intelligence collection) essential to their execution. To begin, we need to develop the equivalent of what the military calls an "order of battle" on foreign intelligence services of concern. These are positive intelligence requirements, which include answering such questions as:

- What is the American targets capability of the adversary service? (Foreign intelligence services have a set cadre of personnel trained to go after American targets; U.S. counterintelligence needs to understand who they are and how they operate.)
- What is the doctrine by which the service deploys?
- What are its budget, training, personnel records?
- What are its liaison relationships, and what are their resources and targets?
- What are the critical nodes of foreign collection against us?
- What are the signatures of the intelligence precursors to an attack?
- What is their leadership structure?
- How and by whom are they tasked?

Nations use their intelligence services for particular purposes that are as diverse as the national ambitions they support. In exploring these questions, we should not be surprised, therefore, to see intelligence officers from different services trained and deployed in signature ways.[39] Just as we are learning to map the networks of terrorist groups, so too can we analyze the ways in which foreign services are built and operate. This analytic work, in turn, should lead to refined collection requirements to fill in the blanks in U.S. knowledge and to support strategic operational planning to exploit foreign intelligence vulnerabilities.

It is the clear objective of the National Counterintelligence Strategy that the United States should never again have to deal with the intelligence services of another hostile country from a position of near ignorance. The challenge is to develop a common operating picture and operational insights into the target services, as well as plans and capabilities to degrade them as our national security requirements dictate. The benefits will be many: in wartime, we will be ready, and in peacetime, we gain advantage to protect lives, shape threats, defuse dangers, provide insight into warning of war, and protect our national security secrets.

Protect Critical Defense Technology. The National Counterintelligence Strategy directs that U.S. counterintelligence help protect the vital technology secrets that are the bedrock of our strategic security. America's deterrence and defense have long depended on strategic secrets: the locations of our hidden retaliatory forces, the codes by which we protect our military and diplomatic communications, the intelligence sources and methods that give us warning and permit us to understand the threats and opportunities we face, and the sensitive technologies that give us military and commercial advantage. The United States cannot maintain its dynamic technological superiority without a corresponding counterintelligence superiority.

A national defense strategy based on "transformation"—the ability to develop and incorporate transformational capabilities, technologies, and techniques that render adversary capabilities obsolete—places a premium on the sensitive capabilities and technologies that give advantage. The single most effective strategy to defeat U.S. national defense plans to ensure superiority through transformation is to capture those essential secrets in order to incorporate them into adversary weapons systems and to develop countermeasures. Foreign militaries that acquire controlled U.S. technologies are able to leapfrog technological barriers that would otherwise slow or even prevent the production of more sophisticated weapons.

Espionage has long proven the most cost-effective means of defeating U.S. capabilities. We may spend billions of dollars to develop a given weapons system, the effectiveness of which rests on essential technological, operational, or design secrets that give us advantage. If those essential secrets are stolen, both our investments and our advantage can be lost. The cost-benefit ratio of espionage is sharply in the adversary's favor.

Accordingly, the covert acquisition of U.S. technology has long been a goal of most foreign intelligence services as well as other foreign entities. The insights Farewell provided into Soviet technology acquisition operations indicate the level of resources that adversaries are willing to commit to the effort. Following in Russia's footsteps, China has acquired surreptitiously key technology for its military modernization programs from the United States. While not alone in the technology acquisition business, China is surely in the top tier of the most active and effective:

- In the last 10 years, China has remained among the top intelligence threats because of its strategic intent to counter the United States, its increasingly sophisticated capabilities, and its abundant opportunities to gather U.S. data. China's intelligence interest in U.S. personnel is growing, owing to such things as the war in Iraq, North Korean belligerence, and increased tension over Taiwan.
- China maintains some of the world's most effective intelligence services—including the Ministry of State Security and the People's Liberation Army Military Intelligence and Technical Intelligence Departments—with global reach.
- Collection of scientific and technological information has been one of the Chinese intelligence services' top priorities. In recent years, China has successfully used espionage to acquire a range of sensitive U.S. technologies, including design information on all of the most advanced U.S. nuclear weapons, missile design and guidance technology, electromagnetic weapons R&D, and space launch capabilities.[40]
- In addition to more familiar techniques, China's use of nontraditional intelligence methods, including an extensive network of collectors who are not professional intelligence officers, has enabled it to operate with less scrutiny from U.S. counterintelligence.

The most successful espionage—the kind that goes undetected—is all the more effective because what is not known cannot be remedied. And the risks are growing. The marvels of modern information technology and microelectronics have revolutionized espionage tradecraft, enabling the clandestine extraction of vast volumes of data in miniaturized storage media or across computer networks with a keystroke.

The Nation looks to counterintelligence both to give insights into the foreign intelligence threats against technologies vital to our security and to supply options to counter those threats. That job requires focused and creative CI collection activities, strategic analytic exploitation, and coordinated operational discipline.[41] But in the absence of an overall integrating and consistent policy to stop technology diversion, the work of counterintelligence will be only a drop in a leaky bucket.

It is difficult to determine how much of the theft of sensitive U.S. technology and intellectual property is being directed by foreign governments, rather than self-initiated by businessmen, academics, or scientists for purely commercial or scientific reasons. Anecdotal evidence and incomplete statistical information indicate that much trade secret and technology theft takes place without direct intervention by foreign governments, although most foreign governments that are involved do not discourage such activity and themselves benefit from the transfers. Consequently, protecting the U.S. sensitive technology base from foreign diversion is inherently a multifaceted undertaking, involving export control laws, diplomacy, international conventions, intelligence, public education, demarches, interdictions, as well as counterintelligence.

U.S. counterintelligence has the job of identifying those operations in which a foreign intelligence hand is orchestrating efforts to acquire sensitive U.S. technologies. However, the key to protecting America's qualitative defense advantage is to draw upon all the tools of statecraft, national policy, law enforcement, and public awareness to deny adversary acquisition of essential technology secrets. These things must be done in concert, if they are to succeed, and that is a policy call.

Defeat Foreign Denial and Deception. Ancient Biblical wisdom, "On your own intelligence rely not" (Proverbs 3:5), underpins the fourth strategy pillar: U.S. counterintelligence shall safeguard the integrity of intelligence and identify and defeat foreign denial, deception, and covert influence operations.

Analysis of foreign denial and deception (D&D) activities is arguably among the most challenging of intelligence analytic disciplines. Throughout history, nations have sought advantage over rivals through the manipulation of valued information. Such manipulation spans a spectrum of activities from the simple act of keeping certain information exclusive or secret to sophisticated deceptions that seek to confuse or mislead an adversary's collection, analytic, and decisionmaking process. This spectrum includes *denial*, in which information is used in a "defensive" way by keeping it both secret and hidden (where the information gains further advantage through exclusivity and obscurity), and *deception*, in which information is used in an "offensive" way to mislead or confuse an adversary and which can include the use of both truthful and overt as well as false information in such a way as to influence a rival nation's perceptions. The discovery and uncovering of the first, and protection against the second, are "the two great purposes of intelligence."[42]

While the first key purpose of intelligence—the identification, gathering, and accurate interpretation of a foreign nation's secret information in order to gauge its intentions and capabilities—is difficult, particularly where the very existence of the information is hidden, the other key purpose—guarding against deception—is even more challenging. Deception analysis focuses on providing a type of quality check on the information gathered about foreign nations in order to uncover the purposeful falsehoods sent out by nations seeking to gain advantage. In most cases, nations use denial and deception in combination, further compounding the challenge to collectors, analysts, and decisionmakers. Indeed, denial and deception are inextricably woven. Nations historically—and currently—have employed D&D as an organic whole, therefore placing a premium on sophisticated and nuanced all-source analysis for its detection and understanding.

The ever-present possibility of deception is "a dilemma and predicament of intelligence work."[43] All intelligence services practice deception, from the mundane practices of lying and falsifying documents to elaborate double and triple agent operations to the exploitation of channels of communications known to be compromised. Adversaries (and even friends[44]) attempt to mislead U.S. intelligence and sway decisionmakers. The more they know about U.S. intelligence, the greater their chances for success.

Our political strength also turns on protecting our institutions and alliances from covert influence operations by foreign intelligence services. Thanks to the information revolution and the explosion of technology, the technical potential to influence perceptions is extensive and growing, as is our susceptibility to such techniques. Also increasing is the number of channels through which influence may be exerted, through both clandestine intelligence channels and open sources of information.

Successful foreign penetrations, both human and technical, have netted foreign intelligence services an enormous amount of U.S. classified information, enabling debilitating countermeasures to U.S. intelligence collection and analysis. One of the greatest bargains in espionage history was the Soviet purchase of the technical manual for the KH–11 reconnaissance satellite from former CIA employee (now convicted spy) William Kampiles for a paltry $3,000. As a result of this theft and other compromises, U.S. intelligence must assume as a matter of course that overhead imagery and other technical collection will be met by D&D efforts.

There is a continuing market for these stolen U.S. secrets, which can be sold or bartered to third party states or terrorist organizations that have their own uses for the information. The knowledge gained of U.S. intelligence sources and methods—through spies, unauthorized disclosures, and even some authorized disclosures—has aided in extensive concealment and denial programs that increase our uncertainty about foreign capabilities and intentions, and more effective foreign deception operations to mislead us. India's detonation of nuclear explosions in 1998, which came as shock to U.S. intelligence, was a prime example of such a successful effort.

As a result of sensitive knowledge gained about U.S. intelligence, many nations have learned denial and deception techniques to present a false picture of reality. These foreign D&D practices may lead U.S.

analysts to faulty judgments, when vital information has not been collected, or when deception distorts understanding. The danger is that useless or deceptive information—whether from human or technical collection—may be integrated into U.S. intelligence and disseminated to policymakers, weapons designers, warfighters, and even the warning community as if it were true.[45]

Modern technology compounds the avenues for deception, but the problem is one that was known to the ancients. The notion that "all warfare is based on deception" dates from the 6th-century BCE writings of Sun Tzu, who devotes the closing pages of *The Art of War* to the classes and value of spies, how to convert enemy spies to one's own service, and how to use "doomed spies" as double agents "to carry false tidings to the enemy." He tempers these instructions to the successful general with the strong caution that the use of spies to deceive and mislead is a two-way street, and that "without subtle ingenuity of mind, one cannot make certain of the truth of their reports." It is the enduring job of counterintelligence collection and analysis to supply that "subtle ingenuity" to protect and validate U.S. intelligence, and in so doing to reveal otherwise unseen strengths and weaknesses and threats that adversaries pose.

Level the Economic Playing Field. U.S. companies are competing in an increasingly challenging global market and occasionally against foreign competitors who may have an unfair advantage at their disposal: the hidden resources of their governments. Of particular concern, when it comes to commercially valuable financial and technical information, private American firms may find themselves competing not only with other companies but also, on occasion, against foreign intelligence services. For example, Pierre Bousquet de Florian, chief of France's internal security service, openly declared at the end of 2003 that business intelligence was a major priority, along with the fight against terrorism. Other states may be less candid but even more aggressive. The National Counterintelligence Strategy directs that U.S. counterintelligence work expose these foreign intelligence practices in order to help ensure a level economic playing field for U.S. business and industry.

The protection of American strategic information and technology, including the proprietary commercial information that brings competitive advantage, has long been an element of the Nation's security. Lead responsibility for that job falls to the private sector owners of that information and technology, but government also has a role to play, and U.S. counterintelligence has a job to do.

As a first and obvious step, government can provide information about the threat, to the extent that intelligence is available and can be confidently shared. Of course, information-sharing is a two-way street. The most immediate tip-offs to foreign economic espionage activities usually come from such things as industrial plant incident reports, overly inquisitive foreign merchants at international trade shows, or the experiences of businessmen who return to their hotel room to find their laptop missing along with the proprietary data on its hard drive. The commercial sector's willingness to share such information with the government depends in turn on its confidence that the government is able to protect commercially sensitive data and that the information provided will be put to good use.

The intimate interplay of security and counterintelligence in managing risk underscores the importance of a close government-industry relationship. U.S. counterintelligence has the job of identifying foreign intelligence operations, including the way foreign governments may use intelligence resources to gain commercial advantage. But it is up to business and industry to decide how to protect themselves against these potential threats. No enterprise can be completely secure, so U.S. business and industry will always face some level of risk; deciding how to manage that risk to carry out operations effectively is the real security challenge. In that effort, counterintelligence and security cannot be afterthoughts imposed on corporate R&D personnel, businessmen, or mid-level managers. Heightened awareness and intelligent security practices that protect the valuable secrets of the corporation are the best guarantors of success against the foreign intelligence threat.

The U.S. Government, and particularly the Department of Homeland Security, has a concerted effort under way to ensure the availability and accessibility of essential threat information to critical infrastructure owners and operators, as well as state and local authorities responsible for security and other protective measures against terrorist threats. While the government's principal focus must remain the terrorist

threat, there is also room to enhance outreach to the private sector to increase awareness of the economic intelligence threat facing the Nation as a whole. In particular, U.S. counterintelligence can provide threat information and help educate the science and technology community to the variety of ways foreign adversaries may employ intelligence techniques to steal information.

Inform National Security Decisionmaking. The National Counterintelligence Strategy directs that the national security decisionmaking process be informed by the particular insights that counterintelligence can provide. For example, it is no secret that Syrian intelligence and security services are integral to President Bashar Assad's power. As our national security leadership considers how to deal with Syria, it might be helpful to explore the following questions:

- What would cause those services to withdraw their support for Assad?
- Is there a residual Syrian intelligence capability in Lebanon, left behind in the wake of the withdrawal of Syrian troops? If so, what role is it playing, and how does it interact with Hezbollah?
- Is Syrian intelligence involved in supporting other terrorist groups? If so, which ones and how?
- Is Syrian intelligence supporting insurgency operations in Iraq? If so, who specifically is responsible?
- What is the level and nature of Syrian intelligence cooperation with Iran?
- Does Syria conduct clandestine operations in Europe or in the United States?

For the future, the President is looking to the Director of National Intelligence, the National Counterintelligence Executive (NCIX), and the CI community to be ready to answer questions such as these.

As a new guest at the policy table, counterintelligence should be prepared to present an array of strategic CI insights and operational options in foreign and defense policy for the President and his national security leadership team. The tasking or operations of foreign intelligence services as a tool to achieve adversary objectives are of no small interest to national security policymakers in understanding and addressing this "secret war" dimension of foreign power. In turn, U.S. counterintelligence must look to the policy leadership to prioritize the questions and objectives that will drive the allocation of CI collection, analysis, and operations.

Build a National Counterintelligence System. The final pillar calls on the departments and agencies with CI responsibilities to design and equip the new elements, plans, and processes necessary to execute the National Counterintelligence Strategy—in effect, to turn the vision of what needs to be done into the reality of what we can do. And therein lies the real challenge. As the reader may conclude from the summary above, the National Counterintelligence Strategy is a prescriptive narrative of how counterintelligence should support national security strategy. The question is, why does it not work that way now?

Bringing a Strategic Approach to U.S. Counterintelligence

In explaining why he thinks Americans do not do strategy very well, Edward Luttwak observed that, as a nation, our strengths generally lie elsewhere:

> Americans are pragmatic problem solvers rather than systemic or long range thinkers. Our whole experience tells us that it is best to narrow down complicated matters so as to isolate the practical problem at hand, and then to get on with finding a solution. Strategy by contrast is the one practical pursuit that requires a contrary method: to connect the diverse issues into a systematic pattern of things; then to craft plans—often long range—for dealing with the whole.[46]

Similarly, personal experience suggests that America's FBI agents, or our military investigators, or our case officers at CIA, do not readily appreciate the relevance of big-picture national strategy to their daily work. The training and mental discipline needed to master the specifics of a case, the voluminous details of an investigation, the intricacies surrounding an asset's recruitment, handling, and reporting, all focus on the practical objective at hand. The CI professional's caseload is developed, assigned, and managed within the well-established channels and authorities of the cognizant agency, and his or her performance is evaluated by their exacting standards.

But U.S. adversaries do not target an FBI field office, or a CIA station, or a military unit. They target the United States. In other words, while the foreign intelligence threat is strategic, the history of U.S. counterintelligence has been one of dividing responsibilities in order to be able to address foreign intelligence threats pragmatically, rather than dealing with the strategic whole.

A History of Fragmentation

When the U.S. Intelligence Community was organized in 1947, it was clear from the start that a single leader was essential to bring coherence to its many components so the enterprise could be responsive to national direction and national security needs. The Director of Central Intelligence was created to provide that leadership, and recent law has strengthened and expanded the post to the new position of Director of National Intelligence.

By contrast, until very recently, the U.S. Government did not take a strategic view of counterintelligence. Its 60-year history has been one of having no one in charge of the enterprise. Counterintelligence had no central leadership because it was seen not as a cohesive undertaking, but rather as a complicated set of threat-driven pragmatic activities, each of which was measured on its own terms, not by 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 good things that can make for fabulous stories revealing flashes of brilliance, creativity, and daring, and heralding some true legends in the business.

Far rarer is the case in which the operational possibilities of ongoing investigations, 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 wired to work that way.

Historically, the CI community was not organized or structured to accomplish a central national mission; rather, its various elements have grown out of individual department or agency responsibilities, with operational authority split in gross terms between the needs of domestic security against foreign agents (FBI), and the operational needs of intelligence collection (CIA) and military actions in the field.[47]

Federal Bureau of Investigation. The FBI became America's leading CI agency as a result of the cumulative series of authorities, responsibilities, and skills that it acquired in response to changing national needs over the course of the last 90 years. 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. This long and episodic history is both a blessing and a curse. It has given the Bureau the premier standing it has today among the Nation's CI agencies, while also straining its ability to keep pace with expectations.

When German saboteurs began operating within the United States during World War I, there were no laws against domestic espionage or sabotage and no lead agency for domestic security. One contemporaneous report counted 43 suspicious fires or explosions at war materiel plants from 1915 to 1917, bombs on nearly 50 U.S. ships carrying supplies to the Allies, and hundreds of lives lost to German agents who had infiltrated the United States.[48] The country turned to Federal law enforcement to investigate and stop the saboteurs.

Upon America's entry into the Great War, Congress passed the Espionage Act and assigned its enforcement to the 400-member Bureau of Investigation in the Justice Department—the precursor of the FBI. In the mid-1930s (when Charles Burton Marshall was fresh out of college), President Franklin Roosevelt, prompted by concern over the growth of domestic movements supporting communism and fascism, secretly expanded the FBI's jurisdiction over domestic intelligence. Throughout World War II, the Bureau concentrated on Axis espionage threats within the United States as well as Nazi intelligence operations throughout Latin America. When the structure of the Intelligence Community was formalized in 1947, the FBI's 20-plus-year history in domestic security (intelligence, countersabotage, and counterespionage) resulted in its de facto assignment as lead agency for counterintelligence (which was defined as including all of these things).

Since then, the FBI has evolved through several distinct stages in the execution of its CI mission.[49] From at least the 1960s through the early 1980s, every agent in the National Security Division, where CI responsibilities are lodged, knew that his central job was to recruit KGB personnel. At that period in the Nation's history, a clearly defined adversary eclipsed all other intelligence threats, and there was a correspondingly clear mission to penetrate that threat. The FBI also conducted CI operations against known and suspected intelligence activities of a classified list of so-called criteria countries, namely the communist nations.

With the issuance of Executive Order 12333, "United States Intelligence Activities," in 1981,[50] the FBI was explicitly directed to conduct and coordinate all CI activities within the United States. As a result, in the ensuing years of the Reagan administration, CI's share of the Bureau's resources increased from about 10 percent of the agent workforce up to nearly a quarter. The FBI's central strategic focus shifted to counterespionage—finding foreign penetrations into the U.S. Government. The "Year of the Spy" in 1985 and the flood of espionage prosecutions in the years that followed were visible successes of the FBI's work.

Then, the Berlin Wall fell, and an abrupt drawdown in resources occurred across the Intelligence Community. The National Security Division fell back to the 10 percent mark of the FBI workforce, where the CI division remains today. The old criteria country list was overtaken by events. Searching for a method of ordering CI operations in a time of multiple and uncertain foreign intelligence threats, the FBI adopted a new National Security Threat List to prioritize its CI work, which took into account foreign activities in the United States as well as a range of things of strategic importance to the country's security and economic well-being.

The Nation was hit by the first World Trade Center attack in 1993, followed by the deadly bombing in Oklahoma City in 1995. For the FBI, these shocks meant an influx of funding to combat terrorist threats, as well as new demands on leadership attention and expectations for Bureau performance.

Then came September 11, and in its wake came the creation of a new National Security Branch at the FBI, dominated by the counterterrorism mission. As a result of new national priorities, the non-terrorist-related CI programs have become a reduced collateral mission, focused largely again on counterespionage.

Despite recent changes, the FBI remains first and foremost a law enforcement agency, responsible for investigating violations of Federal criminal statutes, including the Espionage Laws.[51] Much of its counterintelligence expertise is derived from the techniques and training required for such criminal investigations. Ask any FBI agent working counterintelligence, "Are you principally an intelligence officer or a law enforcement officer?" 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. But there is no question that the Bureau's responsibilities have evolved from a relatively narrow counterespionage focus to those of a full-scope counterintelligence service for virtually all foreign intelligence activities occurring within the United States.

Central Intelligence Agency. The history of U.S. counterintelligence abroad is far different. Following a 2-year interregnum after the disestablishment of the OSS, the newly created CIA inherited several components largely intact from their predecessor: a research and analysis function; a covert action staff; a clandestine HUMINT arm (originally known as the Directorate of Plans, later Operations); and a separate counterintelligence staff (known as X–2 within OSS) within the Directorate of Operations (DO). The focus of this CI staff was the conduct of certain CI operations and CI review of DO operations. Other than to include counterintelligence as part of its definition of intelligence (foreign intelligence being the other component) and to exclude the CI activities of the FBI from its definition of national intelligence, the National Security Act, which established the CIA, gave no particular CI responsibilities to the agency.[52]

Against the backdrop of the Cold War and the activities of the KGB, counterintelligence developed within the CIA largely as a component designed to protect offensive clandestine operations from compromise. In 1974, a complicated 20-year history of conceptual, bureaucratic, personal, and ideological struggles within the DO culminated in a purge of the CI staff following public revelations of CIA improprieties. These events led directly to the 2-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, the Agency effectively withdrew from even its narrow CI mission and has been on a long road to recovery.[53] The revelation

of Aldrich Ames' devastating 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 within 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.

The essential point is this: CIA was not directed and 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. Far from being a partner with the FBI to build a global perspective on the operations of foreign intelligence services, the CIA has interpreted its CI job as confined to protecting its own house and mission. During the Cold War, the DO 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 the Agency has never seen itself with a comprehensive overseas CI mission corresponding to the mission that evolved for the FBI domestically.

Department of Defense. War planners understand the necessity of neutralizing the intelligence capabilities of the adversary. As General George Washington famously said, "There is one evil I dread and that is their spies." Accordingly, counterintelligence as a military mission has long been counted among the war arts.

But in peacetime, counterintelligence (including counterespionage) at the Department of Defense (DOD) is grounded in the larger force protection mission of the military services. Each of the Services charters and organizes its relatively narrow counterintelligence efforts substantially differently according to 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.[54] As is common to other functions within the hierarchical DOD organization, each combatant commander also has a CI staff element, while the Services organize, train, and equip their CI components assigned to support the combatant commands.

With each of the Service components attending to its own needs, no entity was charged with the CI concerns of the many independent defense agencies, activities, and non-Service personnel, nor was there an entity 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 begin to redress this deficiency, the Counterintelligence Field Activity (CIFA) 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. CIFA's charter, however, does not confer any authority to conduct operations or investigations, and CIFA is still enduring the growing pains of a new umbrella organization trying to establish its responsibilities at home and abroad and to impose order over formerly (and still mostly) independent entities with long histories.

Although DOD owns or controls most of the secrets worth stealing, it does not command the 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 the agencies that have lead CI responsibility in those domains—CIA and FBI, respectively. Nor does the Reagan-era Executive order assign DOD or any of its sister agencies the duty of forging an integrated CI mission to protect the United States against foreign intelligence threats.

What's Wrong with This Picture? The problem is straightforward. Historically, the Nation's CI capabilities have grown from the bottom up rather than being planned from the top down. As a result, U.S. counterintelligence consists of five operating arms that are a loose confederation of independent organizations with other and varying responsibilities, jurisdictions, and capabilities. Their operations have tended to focus on individual cases, with little appreciation of the potential impact of a synergistic effort. While bilateral interaction between sister agencies has increased in recent years and especially in the wake of September 11, taken together those contacts do not begin to equal a cohesive, integrated whole.

It is not a question of needing better management over U.S. counterintelligence. Rather, it is a basic design flaw in U.S. counterintelligence, in which the whole is less than the sum of its parts. Individual CI collectors, investigators, operators, analysts, and support personnel can and do perform extraordinarily well, but taken as a whole, their efforts fall far short of potential and need. Individual agents, investigators, or intelligence officers can be very proactive and exercise great initiative and creativity, and yet the sum of what they do will not bring us a strategic offensive gain against foreign intelligence threats unless orchestrated to a common purpose.

Without an overarching national CI mission to prioritize threat and articulate goals and objectives, or a national mission manager to program, conserve, and orchestrate CI activities, the operational elements have been left to manage their work product to serve their individual ends, creating inherent seams that invite foreign exploitation. Many of the counterintelligence deficiencies that have cost us so dearly have been the result of this systemic failure in the architecture of U.S. counterintelligence.

A New Architecture for U.S. Counterintelligence

Even before the September 11 attacks, U.S. counterintelligence was in a period of transformational change as a result of the dramatic CI lapses of the last 15 years—a long series of devastating espionage cases that have continued to the present (see figure 2). Some of the damage done by these traitors can be attributed to protective security vulnerabilities that they were able to exploit. But these losses also represent a strategic failure of our nation's CI capabilities.

Many of the antecedents to this strategic CI failure reflect the same kinds of gaps and deficiencies identified in the post-9/11 review of U.S. intelligence failures. In particular, the FBI and the rest of the CI community have been criticized repeatedly for failing to collect useful intelligence, to analyze strategic intelligence, and to share intelligence internally and with other members of the Intelligence Community. Since the FBI is the lead counterintelligence organization in the U.S. Government by law and Executive order, its performance of the national CI mission has fallen under particular scrutiny.

Figure 2. Damage from Espionage

Over 118 persons have been indicted or prosecuted for espionage-related offensives since 1974, and caused untold damage to U.S. national security.

Here is a tiny sampling:

- Conrad ring operated throughout the 1970s and into the 1980s. Provided East Germany details of U.S. war plans in Europe
- 18-year long Walker-Whitworth ring supplied crypto key access to U.S. Navy communications (submarine locations, convoy routing) to Russia
- CIA officer Aldrich Ames spied for Russia for 9 years; compromised the identities of virtually all CIA and FBI human sources, many of whom were executed by the Soviets
- Army noncommisioned officers James Hall and David Boone passed Russia detailed data on national technical collection capabilities
- FBI special agent Robert Hanssen spied for Russia for 21 years, suppying highly sensitive national leadership plans and total insight into the FBI's CI capabilities
- During the 17 years she spied for Havana, Ana Montes became the Defense Intelligence Agency's lead analyst for Cuba; compromised all Cuban-focused collection programs, including compartmented activities of broader import
- By unknown hands, China acquired U.S. nuclear warhead designs, enabling them to skip ahead by entire generations
- Recent investigations into other suspected Chinese penetrations into U.S. Government intelligence operations suggest there are even more disturbing revelations to come

Note: See database of U.S. persons prosecuted for espionage or related offenses maintained by the DOD Defense Personnel Security Service, *Espionage Cases 1975–2004* (Monterey, CA: Government Printing Office, 2002), and forthcoming updates at <http://www.dss.mil/training/espionage/index.htm>.

The latest dedicated review of the Nation's CI capability was constituted in the wake of the Aldrich Ames espionage case in order to examine, once again, what was wrong with U.S. counterintelligence. Led by the National Security Council staff in the Clinton administration, the study, entitled "Counterintelligence for the 21st Century" (CI–21), determined that U.S. counterintelligence suffered from two fundamental flaws: there was a strategic CI mission that was not being implemented at a national level, and there was no attempt to coordinate and direct the resources of community members strategically against foreign intelligence activities in the United States.

While there was no serious consideration given to removing the full-scope CI mission from the FBI, the review did result in a series of fundamental changes to the structure of U.S. counterintelligence. Those changes, originally captured in Presidential Decision Directive 75, and then in the Counterintelligence Enhancement Act of 2002, created the National Counterintelligence Executive.[55]

The National Counterintelligence Executive. The central judgment of CI–21 and the Counterintelligence Enhancement Act is clear. There is a national CI mission that is beyond the ability of any individual agency to fulfill. This mission can only be accomplished by ensuring the integration and strategic direction of CI community operations and resources. The law places the responsibility for that coordination on the National Counterintelligence Executive.

The NCIX is the statutory head of U.S. counterintelligence, subject to the direction and control of the Director of National Intelligence (DNI).[56] This executive chairs the National CI Policy Board and heads the Office of the NCIX (ONCIX). The statutory functions of that office include, inter alia, the annual production of the national CI strategy, the identification and prioritization of foreign intelligence threats, the review of all CI budgets and programs against strategic objectives, and the evaluation and professionalization of community performance. The office is also responsible for damage assessments of espionage cases and other compromises of U.S. national security information.

When I was appointed NCIX, the job of providing centralized leadership and strategic guidance to the U.S. CI community was still new, as were the intellectual constructs necessary to provide that leadership.[57] Conceptually, we were faced with three new arenas to define.

First, what is the desired *endstate* for U.S. counterintelligence—what should national CI be able to deliver, and how should it work in a perfect world? To practitioners, this may sound like the excursions of Ivory Tower theorists detached from the real world, but the hard work of thinking through where we want to go is far too often neglected in government undertakings. Having defined clear goals, we can measure progress against those goals. But if we do not know where we are headed, progress reports of accomplishments are not particularly helpful. Within ONCIX, and with the help of some talented senior advisors, we spent a lot of time sketching—and debating—this endstate.

Second, how do we build a national CI system, as directed by the National Counterintelligence Strategy, capable of executing the strategic CI mission? What changes or additions do we need in the U.S. CI enterprise—the many operational and other component programs distributed across the executive branch and the personnel (training, education, skill sets, and duties) who make up our community? This is an iterative process, requiring active engagement and creative contributions from across U.S. counterintelligence. It is also the first task of the planning process to implement the National Counterintelligence Strategy, which was still under way when I left office. While some modest steps have been taken, implementation initiatives to date have not kept pace with identified needs, for reasons discussed below.

Third, how do we constitute an Office of the NCIX to perform the national CI mission?[58] What is the value added of the office to the desired endstate of U.S. counterintelligence, and what is its role within the national CI system? Future incumbents will approach their responsibilities in different and doubtless wiser ways. But as I saw the landscape of U.S. counterintelligence, I found that there were a number of elements missing from the strategic CI mission, which the new office of the NCIX alone could supply. In my view, in order to lead the operational and other components of the U.S. CI community to achieve common strategic objectives, the ONCIX must accomplish a four-part mission:

- supply the center of expertise within the U.S. Government on the foreign intelligence threats to the United States—their "order of battle"—and serve as the national customer to drive collection on those foreign intelligence threats
- ensure that resources and programs across the CI community are developed, allocated, and executed to support collection, analysis, operations, and investigations against foreign intelligence targets as mandated by U.S. national security requirements
- direct integrated strategic operational planning to degrade foreign intelligence capabilities selectively in order to present options to U.S. policymakers
- perform strategic analyses of foreign intelligence capabilities to support national security decisionmakers.

The NCIX is assigned the national CI mission to integrate and provide strategic direction to U.S. CI activities and capabilities in order to identify, assess, neutralize, and exploit foreign intelligence threats to the United States. There is an important distinction between the tactical need for good practices across the CI community and the strategic needs of the national CI program and mission. The CI practices that ensure the security of a given department or agency's operations must be left largely to the discretion of the department or agency. By contrast, in order to perform the national mission, the NCIX must be able to coordinate the considerable resources of the CI community to achieve four objectives: a comprehensive assessment and description of intelligence threats against U.S. interests; the effective and efficient allocation of community resources against that threat; a national CI program to ensure the reliable, timely, and relevant conduct of counterintelligence activities; and an array of strategic operational options and insights regarding foreign intelligence activities of concern to the President and his national security leadership.

These strategic needs of the national mission are new requirements for U.S. counterintelligence. Each of the CI components within the Federal Government has been hard at work at its assigned job. Each CI component, with good leadership, can effect change within its own organization. But it is the overall concept of the Nation's CI enterprise—its architecture and execution—that must change if the Nation is to have a true strategic CI capability. One agency or department acting alone is not competent to do that. The NCIX, under the DNI, must be empowered to lead the way.

Under the old case-driven business model of counterintelligence, which has given us our current fragmented architecture, we are getting about the best we can expect out of our CI programs. For the future, avoiding strategic CI failure will require more than simply doing more of the same. We must draw on the strengths of CI's legacy capabilities but look beyond them to where we need to be. The new strategic approach to U.S. counterintelligence is within reach, but we are not there yet.

Executing the Strategic Counterintelligence Mission. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission), constituted to examine U.S. intelligence in the wake of major failures in the leadup to the war with Iraq, devoted substantial attention to the problems of U.S. counterintelligence.[59] Finding that "the United States has not sufficiently responded to the scope and scale of the foreign intelligence threat," the judgment of the WMD Commission was unequivocally in support of building a strong strategic CI capability and going on the offense.
In particular, the WMD Commission called on the CIA to establish "a new capability" to

> 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.[60]

CIA began to lay the groundwork for implementing this recommendation before Director Porter Goss left office. The newly created National Clandestine Service, under CIA, is ideally situated to deliver, for the first time, a genuine CI capability abroad to complement the FBI's responsibilities at home. It

remains uncertain, however, whether plans for the new external CI cadre will survive in the face of competing demands on the service's HUMINT collection and other clandestine resources.

More than any other single factor, the new strategic approach to counterintelligence will succeed or fail depending on the performance of the FBI in shouldering its newly assigned responsibilities. While the FBI is skilled at enforcing the espionage laws, it is not at present organized, trained, or equipped to collect or analyze intelligence on the foreign intelligence presence in the United States beyond those personnel here under official or journalistic cover. Nor can it develop or execute offensive operations to mislead, deny, or otherwise exploit foreign intelligence activities against us. As the Bureau has concentrated on improving its performance against the terrorist target, it has drawn resources from counterintelligence and fallen farther behind. Yet with 1,720 professional intelligence analysts, and over 12,000 agents capable of collecting valuable information in the field, the FBI is a vastly underutilized resource for countering foreign intelligence threats to the United States. In line with the WMD Commission's recommendations, the consolidation and enhanced professionalization of all of the FBI's national security functions under the new National Security Service, and its effective integration into the Intelligence Community, will be key to the Bureau's ability to deliver a CI capability equal to the modern threat environment.[61] As both the 9/11 Commission and the WMD Commission cautioned, "In the past the Bureau has announced its willingness to reform and restructure itself to address transnational security threats, but has fallen short—failing to effect the necessary institutional and cultural changes organization-wide."[62] The jury is still out on whether this time will be different.

The CIA, FBI, and military Services are working in their separate channels to address different aspects of the foreign intelligence threat with some important linkages between them, but each continues jealously to guard its individual insights and operations, reserving the right to hold them apart from national level cognizance, much less guidance. The job of the NCIX cannot be done so long as there is a gap between the office of the executive and the executing agencies of the U.S. Government. After serving nearly 3 years as NCIX, I know there are many excellent professionals in the ranks of U.S. counterintelligence who understand and support the need for a strategic CI capability and stand prepared to shoulder the new responsibilities necessary to succeed. But there are many others within U.S. counterintelligence and elsewhere in key positions within the Intelligence Community who appear far less enthusiastic about the mission.

The Intelligence Community and Strategic Counterintelligence

The continuing absence of strategic integration and central direction over U.S. counterintelligence presents both opportunities to adversaries to exploit the seams between agencies and barriers to our executing coherent operations against them. The need for a strategic CI capability is compelling, and the law is clear on how the new architecture is to work under the leadership of the NCIX. So what is the problem?

In my experience, the difficulties range from rough spots familiar to anyone trying to effect change in government, to collateral effects from the current upheaval in U.S. intelligence, to specific challenges unique to U.S. counterintelligence. Taken together, these problems present formidable obstacles to accomplishing the national CI mission, but none is insurmountable provided the President's national security team, and especially our Intelligence Community leadership, are united in their support.

First, bureaucracies are notoriously resistant to integrating their work with that of other entities or to accepting direction from an outside organization, especially when they may lose control over their turf. This aversion is magnified when the success of the organization depends in large measure on protecting the essential secrets of its operations. As Ray Cline recalled about the creation of the CIA, "The one thing that Army, Navy, State, and the FBI agreed on was that they did not want a strong central agency controlling their collection programs."[63] Similar agreement exists today among the components of U.S. intelligence and counterintelligence as they regard the DNI and NCIX.

Counterintelligence (and especially counterespionage) breeds an imperative to hold close to information and to stay in control of these extremely sensitive operations and investigations. It can be (and has been) argued that the sorry history of successful, longstanding espionage carried out by trusted insiders is an indictment of the "each is responsible for its own house" approach to counterintelligence. Nevertheless,

bureaucratic resistance to ceding access to sensitive CI information—even the limited information necessary to inform strategic direction—remains fierce.

Government components readily accept and embrace the concept of strategic guidance, provided no one at the national level is looking over their shoulder on operations. The prevailing attitude is, "Tell us what needs to be done; then stand back and let us do it." That approach might work if the national requirements could be met by assigning discrete responsibilities for each operational element, coupled with a mechanism for validating effectiveness of approach and results. But a big part of what is missing in our CI enterprise is the integration of U.S. counterintelligence activities, which entails more than bilateral cooperation between distinct elements. The national CI mission requires the central orchestration of operations against a strategic objective, adding a new dimension of rigor and purpose against which collection as well as investigations and other operations must be measured. Strategic orchestration and integration require more hands-on involvement of the national level office than simply issuing strategic edicts.

Second, it is far easier for bureaucracies to fall back into their comfort zone than to lean forward to meet new demands. It is also easier fiscally to continue existing programs than to end or modify some of them in order to make room for new ones. Instead of strategic consonance, national guidance too often is answered with bureaucratic storytelling to retrofit existing programs against the new strategic template and passive resistance to step beyond such cosmetic measures.

New national level guidance may also be deflected by the retort (genuinely believed by many), "We're already doing that." Despite the searching critique of CI–21, despite the WMD Commission indictments and calls for change, despite the passage of the Counterintelligence Enhancement Act (or perhaps because of these things), there are still many intelligence and law enforcement professionals in the CI business who believe they are already doing all that can be done against the foreign intelligence threat. Perhaps no feature of the National Counterintelligence Strategy or the strategic CI mission has been met with greater misunderstanding in the community than the imperative to go on the offense against foreign intelligence threats.

The foreign intelligence service is the hardest target to penetrate. I have heard senior Directorate of Operations officers disparage the admonition from the WMD Commission and NCIX to take on this target, arguing that foreign intelligence personnel are already at or near the top of the DO targeting list. (Clandestine HUMINT, of course, is not the only collection means of value against foreign intelligence operations.) But 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.

I have also heard senior FBI personnel take strong exception to the implied criticism that the Bureau has not been proactive in the execution of its CI mission. To be sure, the orientation and work ethic of individual FBI agents are very proactive when it comes to working individual cases. But there is a vast difference between the personal initiative exhibited by a law enforcement officer or a CI field unit and the programmatic strategic initiative demanded of the Nation's lead executing agency for CI.

Third, there are a number of factors presently contributing to the continuing neglect of U.S. counterintelligence and the related reluctance among operational components to take on the new responsibilities of strategic CI:

- Homeland security and terrorism concerns currently dominate national policy leadership, commanding their attention and leaving less time for other national security issues deemed of less urgency, such as other foreign intelligence threats.
- The new office of the DNI is preoccupied with the enormous task of constituting itself and the exigencies of effecting changes across the Intelligence Community. Against this backdrop, the national counterintelligence mission is assigned a lower priority than other DNI concerns—a point not lost on the members of the Intelligence Community.
- The FBI is front and center in dealing with terrorist threats within the United States and is concentrating its effort on the counterterrorist work of its new National Security Branch. Having narrowly dodged calls for even greater changes, the Bureau is performing triage and delimiting its CI efforts in favor of attending to counterterrorist investigations. If present personnel and

workload are any guide, the CI performance by the new branch will be measured internally by its counterespionage accomplishments, rather than its performance of the larger strategic CI mission. Time will tell whether the national leadership (the President, the DNI, and Congress) will judge the Bureau's emphasis on counterespionage as sufficient.

- Faced with the fact of the new Director of National Intelligence and the loss of its former status as first among equals, the CIA is uncertain of its own place in the new intelligence order. It is difficult to step up to new responsibilities when the old ones are in flux. Compounding the problem, the Directorate of Operations has been subsumed into the new National Clandestine Service, where counterintelligence is assigned an even lower standing than it previously enjoyed.
- The Defense Department is fighting wars in Afghanistan and Iraq and against terrorist networks globally, in light of which concerns over other foreign intelligence threats have taken on a distinctly secondary role. CIFA, constituted to bring policy and programmatic coherence to the Department's CI efforts, is facing a merger with the struggling Defense Security Service, which threatens to overwhelm what should have been a sleek CI organization with the voracious demands of DOD's security responsibilities. CIFA has also found itself in the cross-hairs of public debate over domestic surveillance, which has led to substantial misunderstanding about DOD's activities in protecting its personnel and programs domestically against foreign terrorist and intelligence threats.
- In addition, the office of the NCIX, which was left vacant for most of 2006, was downgraded upon its incorporation into the Office of the DNI. Without an effective NCIX in office, clearly empowered by the DNI, U.S. counterintelligence has been left with the unmistakable message that it is business as usual.

Fourth, there is an inherent tension between the work of HUMINT collectors and the work of counterintelligence operations. As discussed elsewhere, intelligence collection values above all the information; CI insists on acting on that information, which introduces new risks. For example, if a penetration within a foreign government were used as a CI agent (for example, serving as a channel for deception), that CI operation would introduce a new risk of compromising the asset, to the detriment of the collection effort. Yet the very same organizations that are responsible for HUMINT are also being asked to take on expanded CI operational responsibilities.

In addition, there is a sense in which foreign intelligence capabilities are not regarded as "threats" per se by some of our intelligence professionals, which may seem strange. Indeed, unlike security services that target U.S. collection operations in country, the external intelligence services of friends and adversaries (with few exceptions) are not directed against U.S. clandestine collection, and (until now) no one has been assigned the duty of targeting those services to degrade their operations. There is a sense of competition among intelligence services, but that very competition is more likely to engender a certain professional respect than a perspective that regards the foreign service as a hostile force. The clandestine service looks at its rivals and wants to learn from alternative tradecraft. Adding to this not-quite-a-real-threat attitude, espionage as a generic national security concern has been dismissed more than once with the pseudo-sophisticated pronouncement, "There will always be spies." Such a tolerant view might not seem unreasonable, until we read the file drawers full of damage assessments cataloging the enormous loss in lives, treasure, and pivotal secrets occasioned by spies and other foreign intelligence coups against us. Their content is a cold awakening to what is at stake.

Fifth, offensive counterintelligence in particular can be extremely difficult business, what the classic monograph *A Short Course in the Secret War* deems "an intellectual exercise of almost mathematical complexity."[64] This is graduate-level work, and few are trained for it or intellectually prepared for the task. Consider, for example, the practice of deception. The possibility of deception is an ever-present feature in intelligence work. Alertness to deception presumably prompts a more careful and systematic review of the evidence. But anticipation of deception also leads the analyst to be more skeptical of all of the evidence, and to the extent that evidence is deemed unreliable, the analyst's preconceptions must play a greater role

in determining which evidence to believe. This leads to a paradox: the more alert we are to deception, the more likely we are to be deceived.[65]

Scripting a successful deception effort must exploit the psychological implications of the opposing intelligence service's awareness of the practice. Deception planners must understand its paradoxical nature as well as the many other intricate aspects that make up the psychology of deception to master the demanding nuances of the craft. (So must deception analysts, whose job it is to protect U.S. intelligence from foreign manipulation.) Little wonder that a community already stretched thin on training and education and other resources, and under a microscope for past shortcomings and mistakes, is wary about the prospect of a renewed emphasis on high-risk offensive CI operations.

Sixth, there is a cart-before-the-horse problem in getting the U.S. counterintelligence community to execute the strategic CI mission:

- Without collection against the difficult foreign intelligence targets, there can be no strategic CI operations to degrade them, but
- the Intelligence Community will not turn its resources to collect against the foreign intelligence threat unless Policy (the community of intelligence consumers) so directs; however,
- historically, CI has not been integrated into national security decisionmaking, so Policy is not acquainted with the value strategic CI operational options can supply; yet,
- at the same time, national security leaders have positive intelligence requirements in other areas, which the Intelligence Community must support, so the foreign intelligence target gets assigned a lower collection priority (thus returning to the first point).

To break this impasse, the National Counterintelligence Strategy directs the integration of CI information and operational options into national security decisionmaking in order to educate and inform both communities about threat and opportunity. My experience with CI support to policymakers suggests that it is a supply-side phenomenon, which is to say, if U.S. counterintelligence can supply useful options to Policy, then Policy will want more. It is just a matter of getting started.

Finally, we come to the office that heads U.S. counterintelligence, the NCIX. A very serious problem underscored by the WMD Commission report is that the Counterintelligence Enhancement Act, while assigning specific duties to the NCIX, does not give it directive authority over the CI elements. Nor does it impose a corresponding duty on the elements of the CI community (a term that is itself undefined)[66] to support the NCIX.

To fix this problem, the Director of National Intelligence could 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 that it must have to succeed. Instead, the DNI established substantive deputies to oversee administration, analysis, and collection, with authorities and responsibilities assigned by broad directives within which CI is treated as a lesser included whole. Accordingly, the deputy DNI for administration is responsible for the CI budget, the deputy for analysis is responsible for the CI analytic product, and the deputy for collection is responsible for CI collection priorities. By contrast, the preexisting office of the NCIX was regarded less as an organic element of the DNI's office than an appendage with only such authorities as directly assigned by law. As a result, the CI community is answerable to several entities within the office of the DNI, while to date the DNI has delegated none of his authorities over counterintelligence to the NCIX.[67] Without a strong central advocate, the national CI mission has been put on hold.

Prescriptions for U.S. Policy

It has been said that the trouble with doing something right the first time is that no one appreciates how truly difficult it is. No one who has seriously considered the question of how to bring a strategic approach to the Nation's counterintelligence enterprise will ever lack an appreciation for the difficulty of the job:

> Our [CI] forces are so compartmented that they do not register their aggregate inability to deal with the world-wide coordinated enemy attack. . . . Many of the participants in our effort are also inhibited by

> concern for their particular pieces of the counterintelligence pie in any radical revision of our strategy. Only a recognition of present shortcomings can provide the stimulus for a new effort.[68]

This statement is not a bad assessment of today's CI challenge. It is depressing, however, to realize that these words were written over 40 years ago.

The history of U.S. counterintelligence suggests that fragmentation and lack of strategic coherence will always be the norm. Study after study has recognized the shortcomings in U.S. counterintelligence, and still they persist. Why? I believe what is holding us back is akin to what historian Robert Conquest has called the "dragons of expectation"—the intellectual prejudice and experience-driven belief that legacy institutions are impervious to change and that therefore a new strategic approach to counterintelligence will fail.[69] And yet, there is reason for optimism that those dragons may meet their match.

In 2005, President Bush approved the National Counterintelligence Strategy to go on the offense, and the CI components are responding. Many promising initiatives are under way. The creation of the National Clandestine Service under CIA provides the vehicle for executing the national CI mission abroad, filling a void that has handicapped the U.S. CI architecture from its inception. The creation of the National Security Branch at the FBI 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 CIFA and the ongoing work on CI campaign plans now incorporated within the Department's deliberative planning process.

The office of the NCIX has laid the foundations for executing the national CI mission. It produced the first-ever National Counterintelligence Strategy and the comprehensive threat assessment upon which it is based. It conducted the first community-wide CI budget review, to baseline CI programs against strategic objectives. It has engaged the CI community to build central databases on select foreign intelligence services, which will serve to support strategic analyses and operations and identify collection needs. With the support of the Congress, it has established a pilot project for the CI community to conduct strategic operational planning in a joint environment. It has chartered a National CI Institute to support training and education across the community and to develop common standards for professionalization. And it has established an interagency process for developing the implementation plans needed to execute the national CI strategy and to evaluate and improve community performance.

These are accomplishments of which the CI community justly can be proud—provided they are sustained and carried forward. But these accomplishments, however promising, will be for naught unless three imperatives—without which there can be no strategic CI capability—are achieved.

First, U.S. counterintelligence requires a single leader, with both the responsibilities and the authorities needed to execute that job. This was the philosophy behind the creation of the NCIX, which has become obscured in the wake of the creation of the DNI. Housing the NCIX under a strong DNI should have been a boon to the national CI mission; instead, the DNI bureaucracy has become part of the problem. As the WMD Commission recommended, the NCIX office should be revalidated and empowered to perform the mission it has been assigned.

Second, there should be a national program for CI activities that is strategic, coordinated, and comprehensive as to threat. The national level office needs to have full cognizance of all U.S. CI activities, along with configuration management authorities over the several operating arms including the seminal CI resources of the FBI. Without the power of a common purse, the mission of integrating U.S. counterintelligence to achieve strategic cohesion (much less fielding the new capabilities required by the strategic CI mission) may well be impossible. Unfortunately, the CI portion of the restructured National Intelligence Program (NIP) includes less than a third of the budget and programs formerly subject to central control; fully 70 percent was moved out of the former national CI budget and into Justice and Defense Department budgets or different NIP accounts—a debilitating step back that needs to be reversed.[70]

Third, we need a national CI strategic operations center, a true community operation, to integrate and orchestrate the disparate operational and analytic activities across the CI community to strategic effect. The headquarters staff of the NCIX can lead this effort, but the constituent members of the CI community must man it and make it work. The greatest single void at present arises from the compartmentation of

information such that 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. In the wake of September 11, this incoherence should be unacceptable.

Countering foreign intelligence threats to the United States is a compelling national security mission, much neglected in theory and practice. It is an accident of history that the architecture of U.S. counterintelligence has been fragmented and leaderless, and scores of damaging compromises and missed opportunities have been the result. This flawed approach has endured because of inattention from national security theorists and decisionmakers alike. The time has come for that to change.

Notes

[1] Charles Burton Marshall, "Scholarship and the Real World of the Policymaker," *Orbis* 15, no. 1 (Spring 1971), 283.

[2] A body of scholarship on intelligence has been in the making since Sherman Kent first pointed out its necessity in the mid-1950s, and over the last 20 years, it has expanded to include scholarly writing on strategic intelligence for teaching and understanding international affairs. By contrast, a literature of counterintelligence remains rare even now, and the theme of what does exist is largely confined to examining espionage cases. Most serious writing on strategic counterintelligence in particular is virtually nonexistent. As the director of a large CI organization said to me, "You keep talking about strategic CI. What does that mean?" Kent's words apply to CI today: "As long as this discipline lacks a literature, its method, its vocabulary, its body of doctrine, and even its fundamental theory run the risk of never reaching full maturity. I will not say that you cannot have a discipline without a literature, but I will assert that you are unlikely to have a robust and growing discipline without one." Sherman Kent, "The Need for an Intelligence Literature," *Studies in Intelligence* (Washington, DC: Center for the Study of Intelligence, Fall 1955). I am hopeful that the newly constituted National Counterintelligence Institute will help fill this void.

[3] The first permanent *external* intelligence service, Great Britain's Secret Intelligence Service (SIS), had its origins in the Secret Service Bureau, which was established in 1909 "to counter foreign espionage in the United Kingdom (the Home Section) and to collect secret intelligence abroad on Britain's potential enemies (the Foreign Section). The Home Section was eventually transformed into the Security Service (MI5) and the Foreign Section became the Secret Intelligence Service (sometimes referred to as MI6)." The mission of the SIS is to collect secret intelligence and conduct covert operations overseas. See Secret Intelligence Service Web site, available at <www.sis.gov.uk/output/Page47.html>. As CIA historian Hayden Peake has reminded me, other great powers, notably Russia and Germany, had intelligence services in the 19th century, but they were principally domestic security services with foreign operations to support that mission, rather than external intelligence services in the manner of SIS. One can think of many examples that straddle both functions, but the essential difference is that a security service deals with threats to the security of the state, while the external service conducts collection and other operations abroad to advance and protect the government's defense and foreign policy interests.

[4] For a good overview of the U.S. clandestine service and the meaning of HUMINT, espionage, and covert action, see Norman B. Imler, "Espionage in an Age of Change: Optimizing Strategic Intelligence Services for the Future," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, ed. Roger Z. George and Robert D. Kline (Washington, DC: National Defense University Press, 2004), 219.

[5] Thomas Powers, *Intelligence Wars: American Secret History from Hitler to Al-Qaeda* (New York: New York Review of Books, 2002). Powers sees the present conflict as "a classic intelligence war—one fought mainly with information and the political cooperation of peoples and their governments" (xx). For a different view, see John Keegan, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda* (New York: Knopf, 2003), 319: "Muslim fundamentalism is profoundly unintellectual; it is, by that token, opposed to everything that the West understands by the idea of intelligence."

[6] The earliest recorded use of an agent of influence was by King David, as recounted in II Samuel 15–18. See C.N. Geschwind, "The Tale of Hushai the Archite," *Studies in Intelligence* 13, no. 2 (Spring 1969), 21–24.

[7] David L. Grange, "Asymmetric Warfare: Old Method, New Concern," *National Strategy Forum Review* (Winter 2000).

[8] Robin Winks, *Cloak and Gown: Scholars in the Secret War, 1939–1961* (New York: William Morrow, 1987), 422.

[9] The practical objectives of CI and security are not always in concert, a dichotomy that 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." Christopher Felix, *A Short Course in the Secret War*, 4th ed. (Lanham, MD: Madison Books, 2001), 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.

[10] The term *strategic warning* refers to intelligence about the plans, intentions, and capabilities of an adversary to threaten U.S. interests, while *tactical warning* denotes notification that a specific attack is about to occur or is in progress. For example, in this usage, "Country X is acquiring the capability to attack" is strategic warning of attack, while "Country X is launching an attack" is tactical warning.

[11] Jack Davis, *Improving CIA Analytic Performance: Strategic Warning*, Occasional Papers 1, no. 1 (Washington, DC: The Sherman Kent Center for Intelligence Analysis, September 2002).

[12] U.S. House of Representatives Permanent Select Committee on Intelligence, "Intelligence Authorization Act, FY 1992," report to accompany H.R. 2038, 103d Congress, 1st session (May 15, 1991), 17.

[13] Defense Science Board, *Report of the Task Force on Strategic Intelligence Needs for Homeland Defense*, no. 308 (Fall 2001).

[14] Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999).

[15] Powers, 96.

[16] My thanks to former Deputy Secretary of Defense John Hamre for suggesting these sample questions, which came out of a brainstorming session on how to tie CI more closely to policy needs.

[17] CBS News, *Sixty Minutes*, "FBI Probes Pentagon Spy Case," August 27, 2004; Jeffrey Goldberg, "Real Insiders: A pro-Israel lobby and an F.B.I. sting," *The New Yorker*, July 4, 2005; Mark Thompson and Brian Bennett, "A Reporter's Last Battle: Why the FBI Wants to Search the Private Papers of the Late Investigative Journalist Jack Anderson," *Time Magazine*, May 1, 2006.

[18] C.N. Geschwind, "Wanted: An Integrated Counterintelligence," *Studies in Intelligence* 7, no. 3 (Summer 1963), 15. This article, although dated, offers some interesting insights into the differing tradecraft of clandestine HUMINT collectors and CI operations:

> It is the job of intelligence to collect and analyze information. Espionage for this purpose, insofar as it is aggressive, acts only with the objective of getting past the opposing counterintelligence and security forces as uneventfully as possible. Since the gathering of

> intelligence is a secret preparatory function, agents doing it are not supposed to undertake executive action, agitate, or otherwise risk attracting attention. Counterintelligence, on the other hand, is engaged in covert war, all-out and immediate. It has to take action—at home by investigating, arresting, interrogating, doubling, and prosecuting Communist operatives, and abroad by carrying out recruitment, neutralization, harassment, diversionary, and psywar [psychological warfare] operations against their secret service system. These diverse concepts of responsibility for action not only are fundamentally incompatible but call for agents of fundamentally different temperament and attitudes.

[19] Gus W. Weiss, "The Farewell Dossier," *Studies in Intelligence* 39, no. 5 (1996), 121–126.

[20] Ibid. In fall 1986, another 80 Soviet intelligence officers, assigned under diplomatic cover in New York, San Francisco, and Washington, were ordered to leave the country—the culmination of a series of diplomatic and CI moves to curtail Soviet intelligence operations in the United States. See David Major, "Operation 'Famish,'" *Defense Intelligence Journal* 4, no. 1 (Spring 1995).

[21] According to John Lewis Gaddis:

> The contest would range from buildups in nuclear and conventional weaponry through new and openly discussed war-fighting strategies, economic sanctions, the aggressive promotion of human rights, overt and covert support for anti-Soviet resistance movements in Eastern Europe and Afghanistan as well as for opponents of Marxist regimes in Angola, Ethiopia, and Nicaragua, and the vigorous employment of rhetoric as an instrument of psychological warfare, a trend which culminated in the President's March, 1983, claim that the Soviet Union was "the focus of evil in the modern world."

John Lewis Gaddis, "Strategies of Containment: Post–Cold War Reconsiderations," lecture presented at The Elliott School of International Affairs, The George Washington University, April 15, 2004.

[22] Weiss, 124.

[23] The use of strategic deception in peacetime presents its own set of special considerations. Actions taken to manipulate, distort, or falsify information to mislead the enemy may have the unintended consequences of deceiving the public, calling into question core democratic values. The law is unclear and the ethical questions even more challenging when deception may work to save lives and advance freedom; the practical questions concerning the design and employment of deception are no less complex for national security decisionmakers, as well as for members of the press. For a discussion of these and other matters, see "Strategic Deception in Modern Democracies: Ethical, Legal, and Policy Challenges," conference brief compiled by Carolyn Pumphrey and Antulio Echevarria II (2003), available at <www.pubpol.duke.edu/centers/tiss/pubs/Summary.html>.

[24] The use of double agents, which figured so prominently in World War II deception operations under the code name "Double-cross," is a complex and sophisticated counterintelligence technique:

> A double agent is a person who engages in clandestine activity for two intelligence or security services (or more in joint operations), who provides information about one or about each to the other, and who wittingly withholds significant information from one on the instructions of the other or is unwittingly manipulated by one so that significant facts are withheld from the adversary. . . . The double agent serves also as a controlled channel through which information can be passed to the other service, either to build up the agent in its estimation or for purposes of deception [as was the case with *Overlord*].

F.M. Begoum, "Observations on the Double Agent," *Studies in Intelligence* (Winter 1962), 57–72 at 58, 63.

[25] For exciting reading, the story is probably best told by Anthony Cave Brown, *Bodyguard of Lies* (New York: Harper and Row, 1975). But as Michael I. Handel points out, the definitive history of Operation *Overlord* in light of the ULTRA intercepts has yet to be written. See Michael I. Handel, "Intelligence and Deception," in *Intelligence and the National Security Strategist*, 383, note 20. Handel's article is a nice primer on deception: how to do it and how to avoid it.

[26] Quoted in "The Masters of Deception: At England's Bletchley Park, Recalling the Code-Breakers and Illusion-Makers," *The Washington Post*, May 31, 1999, C–1.

[27] Felix, 128.

[28] For the exception that proves the rule, see E.L. Zorn, "Expanding the Horizon: Israel's Quest for Satellite Intelligence," *Studies in Intelligence* 11, no. 10 (Fall/Winter 2001), 33–38.

[29] Alexander Orlov, "The Theory and Practice of Soviet Intelligence," *Studies in Intelligence* 7, no. 2 (Spring 1963), 45–65.

[30] Felix, 121.

[31] John Lewis Gaddis, *Surprise, Security, and the American Experience* (Cambridge: Harvard University Press, 2004).

[32] It is not possible to supply numbers of foreign intelligence personnel in an unclassified paper. But materials declassified by CIA provide at least one historical reference point on Soviet intelligence operations from the mid-1970s: "The scale of the effort that has been made and continues to be made by Soviet intelligence is difficult to exaggerate. Some 21,173 Soviet nationals reside in the 77 non-Communist countries of the world, of whom 5,943 are officials. At least 60 percent of these, or 3,560, are in fact intelligence personnel," for whom the United States was the main enemy. And that does not count the Soviet intelligence personnel then operating illegally or under nonofficial cover, not to mention the contributions from the intelligence services of the Warsaw Pact. Austin B. Matschulat, "Coordination and Cooperation in Counterintelligence," *Studies in Intelligence* 13, no. 2 (Spring 1969), 25–36.

[33] By way of recent example, the U.S. 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 Government.

[34] The FBI has made structural changes and dedicated substantial resources to counter terrorist recruitment, funding, and other operational activities within the United States, including a major effort to develop a strategic analytic capability equal to its counterterrorism responsibilities. The very size of the counterterrorism effort is a telling commentary on the challenges attendant to characterizing and countering foreign intelligence activities, given the far greater numbers and diversity of known and suspected intelligence officers, agents, and operations within the United States.

[35] Office of the National Counterintelligence Executive, *The National Counterintelligence Strategy of the United States* (Washington, DC: NCIX Publication No. 2005–10007, March 2005).

[36] The National Threat Identification and Prioritization Assessment (NTIPA) is a compendium of foreign intelligence threat data, mandated by statute to be produced annually by the Office of the National Counterintelligence Executive and submitted to the President for approval (Counterintelligence Enhancement Act of 2002, 50 USC 904[e] [1]). Community work on the NTIPA (the first of which was submitted in 2004 and approved in 2005) revealed broad challenges in collection and analysis on these difficult targets. Prioritizing foreign intelligence threats is an even more demanding analytic task, depending as it does on the consumer's interests (for example, foreign threats to DO operations in country X or to deployed forces in country Y may be far different from the rank ordering of country threats to U.S. national security information at home) and the

national security context in which they arise (that is, threat priorities do not directly correlate to foreign intelligence capability alone but must be measured against the potential for harm or disruption to U.S. national security concerns and objectives, as prioritized by policy leadership).

[37] Many in the CI community believed the day of the ideological spy had come and gone, but then came Ana Belen Montes. In 1985, Montes joined the Defense Intelligence Agency as an analyst on Latin America. During her 16-year intelligence career, she became DIA's leading expert on Cuba. She was also in the employ of the Cuban government from the moment she entered duty and swore an oath to defend the Constitution until the day she was arrested for espionage in 2001. Unlike most spies of recent vintage, she did not do it for money, which can show up on financial checks, or out of contempt, which can reveal itself in personality profiles and coworker reports; rather, her motivations were ideological. In a free country, how do security personnel and background checks screen prospective employees for their beliefs, while respecting our constitutional values? This is not an easy question to answer but is an especially compelling inquiry in an age of ideologically driven terror networks.

[38] Michael Sulick, "Al Qaeda answers CIA's hiring call," *The Los Angeles Times*, July 10, 2005.

[39] Over the course of 70 years, U.S. and British intelligence acquired these kinds of insights into the operations of the KGB. See, for example, Wayne Lambridge, "A Note on KGB Style: Methods, Habits, and Consequences," *Studies in Intelligence* 15, no. 1 (Winter 1971), 115–121.

[40] "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," 105th Congress, 2d session, 1999, Report 105–851.

[41] One of the difficulties the FBI has encountered in applying CI techniques to protecting critical technologies is the temptation to want to begin by building a database of all the Nation's critical assets as a starting point for strategic CI planning. Such an approach may reflect sound risk management theory, but in practice, the identification, validation, and compilation of the Nation's critical assets is a very difficult (if not impossible) task, given their daunting numbers, inherent sensitivity, and dynamic character. No one would suggest that thwarting bank robbers must begin with an itemization of all of the Nation's banks. Similarly, even if it were possible to identify all of the Nation's critical assets for CI purposes, the number of classified DOD facilities alone in the United States far exceeds the CI resources available to protect them. Once having identified them, then what? We would still be faced with the need to identify, assess, and counter the foreign intelligence threat against these critical assets, and that requires a global, integrated, proactive CI effort.

[42] From one of many memorable and enlightening conversations with Kenneth DeGraffenreid, professor of intelligence studies at the Institute of World Politics, and former Deputy NCIX.

[43] Handel, 379.

[44] For an accounting of British influence operations against the United States in the leadup to America's entry into World War II, see Thomas E. Mahl, *Desperate Deception: British Covert Operations in the United States*, *1939–1944* (London: Brassey's, 1998). Among other things, Mahl recounts how the SIS, under the direction of William Stephenson, counterfeited and passed to the U.S. Government a Nazi map that purported to show Hitler's designs on the Western Hemisphere; an unwitting President Roosevelt made the fake map a featured exhibit in his 1941 Navy Day speech calling for the repeal of the remaining neutrality legislation. The original map and the other deception material may be found in the official history, *British Security Coordination* (London: St. Ermin's Press, 1998). My thanks to British historian Nigel West for this citation.

[45] See James Bruce, Foreign Denial and Deception Committee Vice Chairman, presentation at Cantigny Conference on Counterintelligence (Illinois, October 2, 2003); publication pending.

[46] Quoted in Colin S. Gray, *Strategic Studies, A Critical Assessment* (Westport, CT: Greenwood Press, 1982), 15.

[47] 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 constituted 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 the National Nuclear Security Administration, the CI offices within the several intelligence agencies (the National Reconnaissance Office, National Security Agency, National Geospatial-Intelligence Agency), and other departments and agencies with intelligence missions (Treasury Department, the Coast Guard), a number of DOD entities engaged in classified R&D (the Defense Threat Reduction Agency, the Ballistic Missile Defense Office), and the important CI support functions at the State Department and the Department of Homeland Security.

[48] Quoted in Michael Warner, "The Kaiser Sows Destruction," *Studies in Intelligence* 46, no. 1 (2002), 7.

[49] I am indebted to retired FBI special agent John Quattrocki for pointing out this historical evolution, as well as for many other penetrating insights and long discussions that helped inform my thinking on the subject of strategic CI.

[50] Executive Order 12333, "United States Intelligence Activities," December 4, 1981, 46 F.R. 59941.

[51] The espionage laws found in Chapter 37 of Title 18 of the U.S. Code generally date from World War I and speak of the gathering and delivering of "defense information" to a foreign power, a definition that does not automatically equate to the modern category of classified information. However, a more modern section, 798, specifically criminalizes the transmittal to unauthorized persons of classified information dealing with codes, cryptography, or communications intelligence activities. This strict statute applies whenever the transmittal (or use) is "prejudicial to the safety or interest" of the United States. Other examples of statutorily protected information carrying criminal penalties include diplomatic codes and correspondence (18 USC 952); nuclear weapons information (Chapter 18, Atomic Energy Act); and intelligence agents identities (Section 601, National Security Act). More recently, Congress expanded the FBI's reach and duties with passage of the Economic Espionage Act of 1996 and (more controversially) its investigatory tools under the USA PATRIOT Act of 2003. Last year, the Bureau sought and received concurrent jurisdiction with the Bureau of Immigration and Customs Enforcement over the enforcement of export control laws.

[52] The National Security Act also denies CIA any policy, subpoena, or law enforcement powers or internal security functions. The Director of Central Intelligence, however, was directed to protect intelligence "sources and methods" from unauthorized disclosure, a duty that has devolved to the DNI.

[53] 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 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.

[54] 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.

[55] 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.

[56] The NCIX reporting structure has gone through three evolutions in its short existence. In January 2001, Presidential Decision Directive (PDD) 75 (the last PDD issued by President Clinton) created a board, consisting of the Deputy Director of Central Intelligence, Deputy Secretary of Defense, Deputy Attorney General, and Director of the FBI, to which the NCIX (appointed by the FBI Director) was to report. Superseding the PDD Board structure, the CI Enhancement Act of 2002 established the statutory position of the NCIX, appointed by the President and subject to his direction and control. The Intelligence Reform and Terrorism Prevention Act created the office of the Director of National Intelligence and subordinated the NCIX and her office to the DNI in 2005.

[57] The first NCIX, David Szady, was appointed by the Director of the FBI in 2001, before the law elevated the position to a direct Presidential appointment. His tenure was cut short by the events of September 2001, shortly after which he was recalled to FBI headquarters. The position of NCIX stood vacant until August 2003.

[58] Later, we added a fourth area: How do we integrate the work of the Office of the NCIX into the new Office of the Director of National Intelligence?

[59] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission), Laurence H. Silberman and Charles S. Robb (Co-Chairs), *Report to the President of the United States*, March 31, 2005. See especially chapter 11 on CI, in which the commission recommended empowering the NCIX to do her assigned job; engaging the directed efforts of HUMINT collectors against the American targets officers of high priority foreign intelligence services; giving investigative and operational authority to CIFA; and establishing a national security service at the FBI that would function as an integral part of the U.S. Intelligence Community.

[60] Ibid., 493.

[61] Ibid., see chapter 10. The WMD Commission was highly critical of the FBI's overall performance within the U.S. Intelligence Community, citing, inter alia, shortfalls in analytic capabilities, quality controls, and strategic focus, as well as its failure to interact effectively with the rest of the Intelligence Community.

[62] Ibid., 468.

[63] Ray S. Cline, *The CIA Under Reagan, Bush, and Casey* (Washington, DC: Acropolis Books, 1981), 112.

[64] Felix, 123.

[65] Michael I. Handel, "Intelligence and Deception," in *Intelligence and the National Security Strategist*, 379, quoting Richard Heuer, "Strategic Deception: A Psychological Perspective," a paper presented at the 21st Annual Convention of the International Studies Association, Los Angeles, California, March 1980, 17, 28.

[66] The Counterintelligence Steering Group, chaired by the Deputy NCIX, invites participation from across the CI community. Current self-identified members include representatives from the Army Assistant Chief of Staff (Intelligence), Air Force Office of Special Investigations, CIA, CIFA, Defense Intelligence Agency, Energy Department, Defense Security Service, Defense Threat Reduction Agency, Federal Bureau of Investigation, Department of Homeland Security, Joint Staff J2, Department of Justice, Missile Defense Agency, National Geospatial-Intelligence Agency, National Nuclear Security Agency, National Reconnaissance Office, National Security Agency, Naval Criminal Investigative Service, State Department Office of Diplomatic Security, State Department Office of Intelligence and Research, Under Secretary of Defense (Intelligence), and the U.S. Coast Guard. The Senior Director for Intelligence on the National Security Council staff is invited to send a representative ex officio.

[67] The title of "mission manager" for counterintelligence belatedly conferred on the NCIX, while a step in the right direction, really does not solve the problem because, by DNI directive, a mission manager's authorities are subordinate to the authorities of the several DNI deputies—each of which has specified responsibilities over CI.

[68] Geschwind, 15.

[69] Robert Conquest, *The Dragons of Expectation: Reality and Delusion in the Course of History* (New York: W.W. Norton and Co., 2005).

[70] Some of the budget restructuring was occasioned by the desire to pull counterterrorism funding out of the FBI's CI budget.

About the Author

Michelle K. Van Cleave was appointed by President George W. Bush to the position of National Counterintelligence Executive (NCIX) on July 28, 2003, where she served until March 2006. As the head of U.S. counterintelligence, the NCIX is charged with providing strategic direction to and ensuring the integration of counterintelligence activities across the Federal Government. Ms. Van Cleave is currently a Senior Research Fellow at the National Defense University and a consultant to Pacific Northwest National Laboratory.

Her prior Government positions include Special Assistant to the Under Secretary for Policy and Senior Advisor to the Secretary of the Army, where she had lead responsibility for homeland defense policy development in the immediate aftermath of the September 11 terrorist attack. She also served under Presidents Ronald Reagan and George H.W. Bush as General Counsel and Assistant Director for National Security Affairs of the White House Office of Science and Technology Policy. She has held staff positions in both Houses of Congress, serving as staff director of the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information; Chief Minority Counsel of the House Committee on Science, Space, and Technology; and defense and foreign policy assistant to Congressman Jack Kemp and the House Republican Conference.

Ms. Van Cleave was of counsel to the law firm of Feith & Zell, PC, and President of National Security Concepts, Inc., of Washington, DC. She is a member of the Board of Directors of the Jamestown Foundation and a member of the bar associations of the State of California and the District of Columbia. She holds JD, MA, and BA degrees from the University of Southern California.

SNSEE FACULTY

DR. R. JOSEPH DESUTTER
Director

PROFESSOR SKEETS MEYER
Dean of Students

DR. JAMES S. ROBBINS
Dean of Academics
Department Head, International Security Studies

DR. THOMAS BLAU
Department Head, Management and Analysis

DR. THOMAS A. MARKS
Department Head, Irregular Warfare

DR. QUERINE H. HANLON
Assistant Professor, International Security Studies

DR. FRANCIS H. MARLO
Assistant Professor, International Security Studies

MR. ROBERT R. REILLY
Instructor, International Security, Specializing in Strategic Communications

MR. ROBERT A. SHARP
Instructor, International Security, Specializing in Stability Operations

MS. MICHELLE K. VAN CLEAVE
Senior Research Fellow

School for National Security Executive Education
National Defense University
Washington, D.C.