Studies in Intelligence Vol. 51 No. 2 (2007)

Strategic Counterintelligence

What Is It and What Should We Do About It?

Michelle Van Cleave

Ever since Sherman Kent's signature work was published, strategic intelligence has been the subject of literature, study, and practice, and, although an author in the pages of this issue of *Studies* will disagree, the subject has come to occupy a well-established place as a core intelligence product line and mission. 1

CIA historian Don Steury has written:

> *In thinking about intelligence, Sherman Kent began with an understanding of national power that was well within the mainstream of contemporary American strategic thought. Kent's contribution was to apply thinking about strategy and national power to an ordered conception of intelligence analysis as an intellectual discipline.* 2

By contrast, "strategic counterintelligence" remains a relatively undeveloped concept, in theory or implementation. Isn't this curious? For if strategic intelligence takes as its touchstone the whole of state interests and the sources of state power, then understanding the purpose and manner in which other states use their intelligence resources to gain advantage and *mastering the capability to counter them* would seem to be the other side of the strategic intelligence coin.

Yet to the extent strategic counterintelligence (CI) is addressed within CI or intelligence circles, it is controversial, poorly understood, and even more poorly executed because it does not fit comfortably within the existing architecture and approach to counterintelligence as it has developed within the United States.

Even though it has been six years since the office of the National Counterintelligence Executive (NCIX) was created to lead and integrate the US counterintelligence enterprise, at present we have neither the ability to perform the mission of strategic counterintelligence nor a common understanding of what it means, much less an appreciation of its value to national security.[a] Indeed, it is one thing to have a national-level office to bring strategic coherence to wide-ranging CI activities, as the law provides; it is quite another matter (to paraphrase Henry Kissinger) to answer the question, "What is strategic counterintelligence and what do you do with it?"

I would like to offer some thoughts on the subject, not to quiet controversy but in the hope of provoking more debate. In my view, the US CI community is at a crossroads. Either strategic counterintelligence is a theoretical construct with little to no place in the real world of US intelligence, in which case we really do not need a national level effort to direct it; or it is a compelling national security mission. If it is the latter, we are losing precious time and advantage and should get on with the job.

The meaning of "strategic counterintelligence"

Counterintelligence has its own distinct logic as an intellectual discipline. As defined at law, counterintelligence embraces both "information gathered" and "activities conducted" to counter foreign intelligence threats.[b]More specifically, it is the job of US counterintelligence to identify, assess, neutralize and exploit the intelligence activities of foreign powers, terrorist groups, and other entities that seek to harm us. Sound security measures are unquestionably vital, but they can only carry protection so far. One can pile on so much security that no one can move, and still there will be a purposeful adversary looking for ways to get what he wants. 3 The signature purpose of counterintelligence is to confront and engage the adversary.

The tradecraft of counterintelligence and its several tactical functions, which are properly within the separate cognizance and competence of units within the FBI, CIA, and the Department of Defense, have well

established objectives and processes that are not at issue here. What is at issue, what the very concept of "strategic counterintelligence" implies, is the potential for engaging CI collection and operations as tools to advance national security policy objectives, and, at the strategic level, to go on the offense to degrade hostile external foreign intelligence services and their ability to work against us.

There are three predicates upon which a strategic CI mission would rest. First, *the foreign intelligence threat is strategic*, meaning that states use their intelligence resources purposefully to gain advantage over the United States and to advance their interests. Second, strategic intelligence threats cannot be defeated through ad hoc measures alone. *The threats must be countered by a strategic response*. And third, *there must be a national level system* that integrates and coordinates diverse programs, resources, and activities to achieve common strategic objectives**.**

The Threat Is Strategic

Foreign intelligence operations against the United States are now more diffuse, more aggressive, more technologically sophisticated, and potentially more successful than ever before. In recent years, we have seen a growing number of intelligence operations within our borders, facilitated by an extensive foreign presence that provides cover for intelligence services and their agents.

Traditional foes, building on past successes, are continuing efforts to penetrate the US government, while waves of computer intrusions into sensitive US government information systems have confounded efforts to identify their sources. We have also seen apparent attempts by foreign partners to exploit cooperative endeavors against terrorist groups to obtain essential secrets about US intelligence and military operations. In addition, a market in US national security secrets has emerged that, among other things, enables foreign practices of deception and denial to impair US intelligence collection. And perhaps most troubling, growing foreign capabilities to conduct influence and other covert operations threaten to undermine US allies and national security interests.

The proliferation of clandestine intelligence services is a striking feature of the modern international security environment. At the start of the 20th century, no state had a standing external intelligence service; today there is scarcely a government that does not have one. And we are only just beginning to understand their modern potential as an extension of state

power.[c]

The use of human intelligence operations by weaker powers to achieve advantage is a classic “asymmetric strategy,” a fashionable term but hardly a new concept. As one student of the concept put it:

> *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.* 4

In the eyes of our potential adversaries, the relative weakness of the United States and its democratic allies clearly is the openness of our societies and people. The opportunity for intelligence officers and their agents to move about freely, develop contacts, and operate unnoticed is no more lost on foreign intelligence adversaries than it was on the 19 hijackers that September morning.

From the standpoint of foreign intelligence interest, there are many potentially valuable targets outside our borders. These would include US government personnel and the far-reaching activities of American commerce and industry. But the real intelligence treasure trove for adversaries is here in the United States.

The central targets of foreign intelligence interest are principally within the borders of the United States:

- The institutions and people responsible for the formulation and implementation of American plans, intentions, and capabilities.
- Intelligence production and weapons design, the secrets of our nuclear labs, and the key R&D activities of our premier industrial enterprises, such as Bell Labs, Boeing, Dupont, and others.
- Thousands of facilities engaged in classified national security work and hundreds of thousands of workers with security clearances dispersed around the country and in most every congressional district.

The CI problem is not only one of sheer numbers of potential targets or foreign intelligence personnel. The larger and more compelling issue is the scope of these activities.

Historically, embassies and other diplomatic establishments in the United States have served as hubs for foreign intelligence activity because of the operational security they afford. Accordingly, the 20,000-member diplomatic community has commanded the lion's share of US CI's 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 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 operational environment of the United States are tailor made for embedded clandestine collection activities. Thousands of foreign owned commercial establishments in the United States, 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 our nation's security.

To cite just one example of the growth in numbers, Russia, reversing a sharp decline that took place during the late Boris Yeltsin's presidency, now has an intelligence presence in the United States equal to its Cold War level, a sizing decision presumably indicative of the return on investment. One need not read too much history to know how successful past intelligence operations against the United States have been. There is hardly an area of national security endeavor that has not been compromised—repeatedly and deeply—by successful espionage.

Strategic threats require a strategically coherent response. Instead of looking at the broader implications of these foreign intelligence operations, we have for the most part adopted a case-by-case approach to dealing with the threat they represented. And by concentrating our CI resources overwhelmingly inside the United States, rather than engaging the foreign intelligence service abroad, we have ceded advantage to adversaries.[d]

Foreign powers have seized the initiative, and moved their operations to US soil, where our institutions are not constituted to work against growing foreign intelligence networks embedded within American society. Here, CI investigations may result in prosecutions for espionage or related offenses, 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 each case at hand and not as part of a larger effort to counter the foreign intelligence service as a strategic target.[e]

As a result, I fear we have neither an adequate understanding of the foreign presence and intelligence operations in the United States nor an appreciation of their broader effects on US national security.

Former deputy defense secretary John Hamre described the challenge succinctly:

> *The goal should not be to catch the spy after he's gotten into the country; we've got to stop him from entering in the first place.* 5

Perhaps we have been coming at the problem from the wrong end. Why wait until foreign intelligence activities show up on US soil, with all the operational advantages of proximity and cover that our rich society provides?

There is another way. US counterintelligence could seize the strategic initiative and begin by working the target abroad, with the purpose of selectively degrading the hostile foreign intelligence service and its ability to work against us. This is the central objective of strategic counterintelligence.

By working the foreign intelligence service as a strategic target globally, US counterintelligence should be able to leverage insights into adversary activities and vulnerabilities to direct CI operations to maximum effect. At home, this means that the operational and analytic focus of US counterintelligence would need to be transformed from its case-driven approach to one that includes strategic assessments of adversary presence, capabilities, and intentions. This in turn would drive operations to neutralize the inevitable penetrations of our government and protect national security secrets and other valuable information.

The National Security Strategy of the United States, and in particular the strategy behind the Global War on Terrorism, embodies just such a national offensive orientation. 6 In times past, the most pressing terrorism-related intelligence question was most often, "who did this?" in turn leading to manhunts, apprehension and rendition for trial. Today the

strategic imperative is to stop the terrorists before they strike, with derivative requirements for operational intelligence support.

Network analyses to map terrorist supply chains, support infrastructures, financial transactions, communications channels, recruitment and training activities, and other footprints serve to focus collection, identify vulnerabilities and inform strategic operational planning to attack, disrupt, and neutralize terrorist operations. While forensic analyses of terrorist acts remain vital, the US counterterrorism enterprise (including its Intelligence Community foundations) is strategically oriented proactively to identify, assess, and defeat terrorist operations.

There is a parallel for thinking about counterintelligence as a strategic mission. Just as US intelligence is mapping the essential features and activities of terrorist groups, so CI analysts could determine how foreign intelligence services are built and operate—call it CI order-of-battle preparation. Key questions would include:

- What is the capability of an adversary intelligence service to target the United States? (Adversary services have cadre trained to go after American targets; US counterintelligence needs to understand who these people are and how they operate.)
- What is the service's deployment doctrine?
- How and by whom is it tasked?
- What is its structure, organization and budget?
- How and where are its people recruited and trained, and personnel records kept?
- What is its leadership structure?
- What are its liaison relationships, resources and targets?
- What are the critical nodes of foreign collection against us?

This analytic work in turn should lead to refined collection requirements to help identify adversary intelligence service vulnerabilities and support strategic operational planning to exploit them—and some thought-provoking new possibilities for advancing US objectives.

The emphasis other states place on human collectors over other means of collection is the single most distinctive asymmetry in modern intelligence structures. This asymmetric reliance on HUMINT has profound implications for US counterintelligence and our national security leadership. If, as part of a broader national strategic plan, we were to have the ability to shape the human source reports our adversaries receive, we may be able to

influence their behavior. 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.* 7

To be sure, this describes an ideal CI operation. But even short of such perfection, by exploiting insights into foreign intelligence activities, counterintelligence can provide new avenues to degrading emerging threats.

Strategic assessments of foreign intelligence capabilities can help inform policy deliberations and frame options for actions. Narrowly, 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. More broadly, there is scarcely an area of national security concern—from Iranian or North Korean WMD activities to Chinese military space activities to fielding effective ballistic missile defenses—that does not have a critical foreign intelligence dimension. When integrated with other foreign policy tools, the insights and operations of strategic counterintelligence operations could make the difference between favorable and unfavorable outcomes in world events.

Let me be clear: Operations to identify, assess, neutralize and exploit foreign intelligence services as a strategic target are not an entirely new concept for US counterintelligence. Over the course of 70 years, US and British intelligence acquired just such specialized insights into the GRU and the KGB, to inform CI operations against the Soviet Union. 8 While not presently configured to work as a strategic whole, US counterintelligence, nevertheless, unquestionably could produce and execute collection strategies to characterize other foreign intelligence services of concern, exploit those sources for their positive intelligence value, and develop options to degrade those services as national security objectives may dictate.

The national CI enterprise must be configured to execute the strategic CI

mission. The strategic CI mission requires a supporting infrastructure to orchestrate the resources of the many parts of the CI community to focus collection and analysis of the foreign intelligence service, perform strategic operational planning to address collection gaps, develop options to degrade the foreign intelligence service, and enable coordinated execution to achieve defensive and offensive CI goals.

This is not CI as it has grown up in the United States. Historically, US counterintelligence has divided responsibilities in order to address foreign intelligence threats pragmatically, rather than strategically. Instead of integration under central guidance at the national level, CI programs have served inherently agency-specific mission objectives.[f] The office of the National Counterintelligence Executive was created to unify the CI enterprise, but these legacy practices remain deeply ingrained.

Counterintelligence is hardwired into CIA tradecraft in order to protect CIA's own clandestine collection and for the purpose of watchfulness against the insider threat (counterespionage). But apart from select activities during the Cold War, CIA has never seen it as part of its standing mission proactively to degrade foreign intelligence capabilities directed against US interests.

The simple fact is that CIA has never been assigned that peacetime mission, and neither has any other operational CI agency. While any CIA officer will tell you that foreign intelligence personnel are already at or near the top of the National Clandestine Service targeting list, it is one thing to check the box for recruitment opportunities, and quite another to have a top down strategically orchestrated effort to disrupt and degrade the operations of a foreign intelligence service.

The FBI is generally responsible for countering foreign intelligence activities within the United States; but despite recent changes the FBI remains first and foremost a law enforcement agency, deriving much of its proven CI expertise from the techniques and training required for criminal investigations. It does not have the people, the organization, training, or equipment to collect and analyze intelligence on the foreign intelligence presence in the United States beyond those personnel here under official or journalistic cover. Neither does it have the capability to develop and execute offensive operations to mislead, deny or otherwise exploit foreign intelligence activities against us. And, in all likelihood, it does not have the public support to venture into the complex grounds of analyzing the vast foreign presence in the United States.

Even the Department of Defense, with its long wartime experience in counterintelligence operations and its highly developed deliberate planning process, has been late to incorporate strategic CI campaign plans as part of standing theater operations plans. 9 In the six months leading up to Operation Iraqi Freedom, an interagency CI strategic planning team came together under DoD leadership to develop a common operating picture of Iraqi intelligence operations worldwide. In response to Command Authority direction, the team was chartered to develop operations to render Iraqi intelligence ineffective.

While this effort, dubbed "Imminent Horizon," resulted in some important successes, the CI community learned its lessons the hard way. Strategic operational planning to degrade foreign intelligence capabilities has long lead times. Beginning at D minus 6 months—as was the case with Iraq—is 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. Defense Department efforts to build on the lessons of this experience have met with halting success to date as a consequence of competing demands on resources within DoD and competing priorities across the CI community.

As a result of this decentralization, CI has evolved into a collection of threat-driven activities, each measured on its own terms rather than for its contributions to a larger whole. 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? These are hard-won CI accomplishments; yet it is far more rare when the operational possibilities of ongoing investigations, or the access of a given penetration, or a double agent tasking, have been fitted against a larger tapestry of the adversary's strategic purpose to inform a CI plan for dealing with the whole. The system is not designed to work that way.

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

and planning—with unknown opportunity and other costs.

What Stands in the Way?

In contrast to the circumstances I have just described, the advantages of having a strategic CI capability would seem straightforward, and the law is clear on how the new CI architecture is to work under the leadership of the NCIX. So what are the arguments against moving apace in that direction?

Maybe we are overstating the threat. In a conversation with me about the concept of strategic CI, an old hand in the British Secret Intelligence Service dismissed it summarily: "You're scaring yourself. The bad guys are nowhere near so formidable as to warrant such a broad undertaking. It's enough to deal with them prudentially; you don't have to go looking for new dragons to slay."

He may be right; but given the changes in the world I noted above, I wonder if it is wise to be so sanguine. What's more, with our nation engaged in a global war on terrorism the threat from adversary intelligence collection has become even more immediate. The need to identify and counter hostile intelligence operations in active theaters of combat is so self-evident that it hardly needs mention. Who would question the strategic value to coalition objectives in Iraq to have a clear understanding and the ability to counter Iranian (and Syrian, al Qa'ida, and other) intelligence activities in that struggling would-be democracy?

And it may well be the case that the best sources on those intelligence operations are to be found not in Iraq but in other parts of the world, another reason why coordinated strategic planning for global CI operations and exploitation to advance theater objectives has been deemed essential (if not yet fully realized).

Even so, espionage as a generic national security concern has been dismissed more than once with the ready pronouncement, "there will always be spies." This view might not seem unreasonable, until one reads 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.

Indeed, the history of counterintelligence reform efforts has been one of

decrying the harm caused by espionage and episodically insisting that US counterintelligence needs to do a better job of protecting against foreign penetrations into our government. How is it that spies within the very heart of US intelligence and the national security community have been able to operate undetected for such unacceptably long periods of time (for example, Aldrich Ames, 9 years; Robert Hanssen, 21 years; Ana Belen Montes, 17 years; Katrina Leung 20, years) to the profound detriment of US national security?

Interagency damage assessment teams are quick to key on exploitable security vulnerabilities and to recommend new security measures (e.g., more uniform polygraph practices, more rigorous background checks, more comprehensive inspection regimes, more sophisticated information system audit trails). But smarter security alone will never be enough so long as the foreign intelligence adversary retains, as he does now, the strategic advantage. The US government may elect to accept the status quo and continue to work against these penetrations one case at a time, but at what cost?

Maybe we are overestimating the value of the target, for its positive intelligence value or operational opportunity or both. After all, the foreign intelligence service is among the hardest of the hard targets. Positive intelligence insights into foreign plans, intentions and capabilities that US decision makers require may more readily be found in the foreign ministries and military war rooms and leadership councils than among their clandestine intelligence officers. And operations to degrade foreign intelligence services may be very difficult and very high risk. At a minimum, adopting strategic counterintelligence is not without costs*:*

- *Resource constraints.* As a national priority, funding for counterintelligence is pitifully low relative to the penalty foreign intelligence successes can exact. While funding for counterintelligence has increased substantially over the past decade, it started that climb from an historic nadir occasioned by the so-called “peace dividend” at the end of the Cold War. The Global War on Terror has diverted funds and national attention that would otherwise have gone to other counterintelligence priorities. Asking the CI components to take on the additional responsibilities inherent in the strategic CI mission would at first blush appear to be fiscally challenging if not impossible. But more money is not the cure, nor is lack of money the problem, so long as the resulting business model of US counterintelligence remains optimized for a defensive posture

of working individual cases at home.

- In time, strategic CI operations should yield insights into foreign intelligence threats that inform US CI activities globally and diminish the adversary's ability to work against us. The FBI should realize the most immediate gains from strategic CI operations as collection against foreign intelligence services abroad begins to fill in the (now largely empty) file folders on intelligence personnel arriving on our shores. In other words, the return on investment in the strategic CI mission should more than offset the cost of redirecting current CI resources and effort; conversely if US counterintelligence does not adopt a strategic approach the marginal return on additional CI dollars is likely to be disappointing.
- *The acute problems of "information sharing."* CIA, the FBI and the military services are working in their separate channels to address different aspects of the foreign intelligence threat, with some important linkages between them; but bureaucratic resistance to ceding access to sensitive CI information—even the limited, sanitized information necessary to inform strategic direction—remains understandably fierce, if not always wise.
- It may be argued that the sorry history of successful, long-standing espionage carried out by trusted insiders is an indictment of the "each is responsible for its own house" approach to counterintelligence. Nevertheless, counterintelligence (and especially counterespionage) breeds an imperative to hold close to information and to stay in control of these extremely sensitive operations and investigations. These ingrained obstacles to information sharing, along with uneven abilities among department and agency representatives to present much less task "blue" side CI resources, make the urgent job of strategic operational planning still one of the great undeveloped interagency arts.
- Fortunately, such reflexive protectiveness commonly is overcome in the field, where people with a shared duty station and purpose are clear that they are working on the same team. Without some way of instilling that spirit and incentive structure in Washington interagency planning groups, strategic operational planning for CI will remain an elusive goal.
- *Operational Risks.* The risks associated with strategic CI are of particular concern to those responsible for clandestine HUMINT. There is an inherent tension between the work of HUMINT collectors and the work of counterintelligence operations. Intelligence collection values above all the information, but CI insists on acting on that

information, which is a very different operational dynamic. 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, which means they must weigh the costs and benefits of the strategic CI mission against their other standing responsibilities.

- Moreover, 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." 10 This is graduate level work, and few are trained or intellectually prepared for the task. Consider, for example, the practice of deception, 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.* 11

- 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 (as must deception analysts, whose job it is to protect US 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 faces the prospect of a renewed emphasis on high risk offensive CI operations with general wariness.
- There is no question that exploiting a foreign intelligence service as a channel for deception or perception management is a challenging task, demanding creativity, imagination, excruciatingly detailed planning and tight execution control. There is, of course, precedent for ambitious operations such as that recounted by the late Gus Weiss in "Operation Farewell." 12

- It was just this kind of high-risk-high-value ingenuity and accomplishment that characterized US intelligence at its inception, pierced the Iron Curtain, and brought us through the Cold War to the position of intelligence dominance we have come to regard as commonplace. Developing the ability to execute the strategic CI mission would at least open the door to these intriguing possibilities.

US CI professionals have made tremendous contributions to the security of our nation. Thanks to their dedicated work there is no reason to doubt that we are deriving about as much value as is possible from the current business model of US counterintelligence. The question is whether our national security leadership thinks that is good enough, because the sum of what our CI agencies do will not bring us a strategic offensive gain against foreign intelligence threats unless orchestrated to a common purpose. That is the mission of strategic CI.

A Status Report

In the final analysis, the decision whether or not to pursue a strategic CI capability is ultimately a policy call. President Bush made the initial call in approving the first National Counterintelligence Strategy in 2005. 13 While broadly a vision statement for the many ways in which counterintelligence should support national security, the strategy's central feature is reorientation of the CI enterprise to enable proactive strategic operations against foreign intelligence threats as national security priorities dictate. The national security leadership has every reason to expect that the CI community is hard at work to deliver this new strategic CI capability.

There have been some important steps forward, and a few back. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, constituted to examine US intelligence in the wake of major failures in the lead up to the war with Iraq, also devoted substantial attention to the problems of US counterintelligence. 14 Finding that "the United States has not sufficiently responded to the scope and scale of the foreign intelligence threat," the judgment of the commission was unequivocally in support of building a strong strategic CI capability and going on the offense. Of particular note, the commission called on 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 US interests. In short, the goal would be for the counterintelligence element to track foreign intelligence officers before they land on US soil or begin targeting US 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. 15

The starting blocks for the strategic CI mission are in place. In line with the commission's recommendation, the 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.

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

Despite these accomplishments, the ability to execute strategic CI operations remains a far-off goal. It is uncertain whether plans for the new external CI cadre at CIA will survive in the face of competing demands on the agency's HUMINT collection and other clandestine resources.

The FBI's performance in shouldering the national security responsibilities it has been assigned is the linchpin to executing the strategic CI mission. But as both the WMD Commission and the 9/11 Commission cautioned, the FBI's past record in effecting institutional and cultural reform to address transnational security threats is not encouraging. 16

CIFA has seen its budget sharply curtailed, and as of this writing its charter and mission are under critical review. Authorities and lines of responsibility over counterintelligence within the office of the DNI are

blurred, while the unity of effort and priority requirements of strategic CI have yet to find expression in ordering the plans, programs, budgets or operations of the component CI agencies. 17

Overall, the most formidable obstacle to progress has been the lack of understanding or consensus behind the purpose and value of the strategic CI mission. Even the end goal behind the creation of the NCIX remains a matter of some dispute. Is the objective to establish a new national capability to execute the strategic CI mission or simply to become more efficient at performing the standing missions of the several CI agencies?

The Bottom Line

Which brings us back to the central question with which this paper began. If the strategic CI mission is a bridge too far as measured against other intelligence priorities, then the DNI and the NCIX need to bring that determination back to the president and the Congress and get on with more promising work. The Office of the NCIX, as the national level CI mission manager, can confine itself to reviewing budgets, plans, and programs against individual measures of effectiveness as put forward by the several CI agencies, look to the training and professionalization of the CI cadre (a very important job), perfect its product line of damage assessments (a solid business area), and continue to turn out annual catalogues of foreign intelligence threats and generic strategy documents that illustrate goals but do not bear responsibility for meeting them. These duties may be quite enough to justify the existence of the office and to validate its value-added as a component within the office of the DNI.

In my view, however, larger national security considerations argue for a purposeful ability to deny, degrade, or manipulate the intelligence capabilities of America's adversaries. If our national security leadership judges that the United States requires such a strategic CI capability, then the DNI, the NCIX, and the whole of the community must step up to that task. That is a much higher bar. But it is not beyond our reach.

Sherman Kent's thinking about strategic intelligence emerged from the historical setting in which he worked, a period which Dean Acheson described in his book *Present at the Creation,* when the national security demands were seen as just a little less daunting than the task in Genesis. There, the challenge was to create a new world out of chaos; "ours,"

Acheson wrote, “to create half a world, a free half, out of the same material without blowing the whole to pieces in the process.” 18 And, as he concluded, it’s a wonder how much was accomplished—advanced by the intellectual rigor of the era’s great strategic thinkers.

Perhaps with the advantage of hindsight, many modern observers have described today’s national security challenges as even more complex than those of the Cold War. Among today’s new realities of strategy and national power are the effective workings of foreign intelligence services in service to our adversaries. At a minimum, we need a clear-eyed evaluation of their meaning for US national security—both the threats they pose and the opportunities they may present—to enable our national security leadership to judge whether the prevailing more-of-the-same response is good enough. This is the intellectual rigor demanded of US counterintelligence today and where the strategic counterintelligence mission begins.

Endnotes

---

[a] The Counterintelligence Enhancement Act of 2002 and Presidential Decision Directive 75 (PDD-75, January, 2001), establishing the NCIX, were prompted by deep concerns over CI’s failure to keep pace with growing foreign intelligence activities that were exploiting seams between the several CI agencies of the US government and targeting not only national security secrets but commercial proprietary information as well.

[b] The definition of counterintelligence found in the National Security Act of 1947 still stands: “information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities.”

[c] The first external service was the British SIS, which originated in 1909. Other great powers, notably Russia and Germany had intelligence services in the 19th century but they were principally domestic security services. 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.

[d] Three-quarters of the US CI budget since World War II has been devoted to activities within the United States carried out by the FBI; most of the remainder, allocated to CIA, the Defense Department, and to small pockets elsewhere in the government, has gone to programs and personnel based wholly or in part within US borders.

[e] One relatively recent example is the espionage case against suspected Chinese agent Katrina Leung, which resulted in a plea bargain in 2005 with no jail time, a $10,000 fine, and 10 debriefing sessions with Leung about her interactions with the Chinese. The US attorney in Los Angeles entered into the agreement because the government's case was not going well in the courtroom, but it effectively forestalled CI efforts to engage Leung's future cooperation.

[f] By contrast, the need for integration and central direction of US intelligence was obvious from the outset; even so, the decades of experience since the National Security Act of 1947 have shown the difficulty of reaching that goal. Imposing a head on an assortment of heretofore autonomous and vastly different CI agencies is a far greater hurdle. As with many national level programs, the good government principle is to know where to draw the line to establish necessary centralization while preserving the freedom of action (including the responsibility, accountability, and authority that come with that freedom) essential to success.

1. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949 Examples of the literature published since Kent's work include: Roger Hilsman, *Strategic Intelligence And National Decisions*. (Glencoe, Il: Free Press, 1956); Bruce Bruce D. Berkowitz and Allan E. Goodman, *Strategic Intelligence for American National Security*. (Princeton, NJ: Princeton University Press, 1989); Richard K. Betts, and Thomas G. Mahnken, eds., *Paradoxes of Strategic Intelligence: Essays in Honor of Michael J. Handel* (London: Frank Cass, 2003); Loch K. Johnson and James J. Wirtz, eds., *Strategic Intelligence: Windows Into A Secret World—An Anthology*. (Los Angeles: Roxbury Publishing Company, 2004); and Loch K. Johnson, ed., *Strategic Intelligence* (London: Praeger Security International, 2007).

2. Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates:*

Collected Essays (Washington, DC: Center for the Study of Intelligence, 1994)

3. The practical objectives of CI and security are not always in concert – which Christopher Felix (TN 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 edition (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.

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

5. Christopher Roache, ed., "Hamre: CI Needs to Accelerate Transformation to Avert Crisis," *The CIFA Track* (DoD: Counterintelligence Field Activity) 20 May 2003: 1.

6. George W. Bush, *National Security Strategy of the United States*, issued in 2002 and updated in 2006. The strategy's emphasis on preemption and preventive measures has made it both distinctive and controversial, but well within the mainstream of traditional American strategic thought. See John Lewis Gaddis, *Surprise, Security and the American Experience* (Cambridge, MA: Harvard University Press, 2004).

7. Felix, 121.

8. For example: "By consolidating information derived from a number of different Soviet sources, it has been possible to reconstruct the process Soviet intelligence uses to spot, screen, train, and assign case officers." Richard Framingham, "Career Trainee Program, GRU Style" *Studies in Intelligence* 10 (Fall 1966): 45. See also Wayne Lambridge "A Note on KGB Style: Methods, Habits and Consequences" *Studies in Intelligence* 11 (Summer 1967): 65–75.

9. See for example James L. Gilbert, John P. Finnegan and Ann Bray, *In the Shadow of the Sphinx: A History of Counterintelligence* (Fort Belvoir: Department of the Army, 2005); reviewed by Michael J. Sulick, *Studies in*

Intelligence 50, no. 4 (2006).

10. Felix, 123.

11. Michael I. Handel, "Intelligence and Deception" in Roger Z. George and Robert D. Kline, eds., *Intelligence and the National Security Strategist: Enduring Issues and Challenges* (Washington, DC: National Defense University Press, 2004), 379, quoting Richards 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.

12. Gus W. Weiss, "The Farewell Dossier," *Studies in Intelligence* 39, no 5: 121–26.

13. Office of the NCIX, *The National Counterintelligence Strategy of the United States* (2005); online at http://www.ncix.gov/publications/law_policy/policy/FinalCIStrategyforWebMa The NCIX is obligated to produce an annual strategy document. According to NCIX Joel Brenner, the 2007 National CI Strategy, recently approved by the president, is intended to build on the earlier effort.

14. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission), Laurence H. Silberman and Charles S. Robb (Cochairmen) *Report to the President of the United States*, March 31, 2005; see especially Chapter 11.

15. Ibid., 493.

16. *Ibid*. See Chapter 10 citing the 9/11 Commission's findings. The chorus of skeptics is growing louder. See e.g., Richard Posner, "Time to Rethink the FBI" *Wall Street Journal* March 19, 2007, A13—the latest in a continuing critique by Judge Posner. For a reply, see Louis Freeh's letter to the editor, "Former FBI Director Says U.S. Doesn't Need a National Police Force," *Wall Street Journal* March 31, 2007, A9.

17. A serious problem underscored by the WMD Commission is that the Counterintelligence Enhancement Act assigned specific duties to the NCIX, but it did not give it directive authority over the CI elements; nor did it impose a corresponding duty on the parts of the CI community to support the NCIX. To fix this, the DNI could simply delegate his directive authority over CI budget, analysis, collection and other operations to the NCIX. This would go a long way toward giving NCIX the authorities and

resources it needs to succeed. Instead, the DNI established substantive deputies to oversee budgeting, analysis and collection community-wide, with authorities and responsibilities assigned by broad directives within which CI is treated as a lesser included whole. As a result, the CI community is answerable to several entities in the office of the DNI, while to date the DNI has delegated none of his authorities over counterintelligence to the NCIX. The title of “mission manager” for counterintelligence belatedly conferred on the NCIX, while a step in the right direction, unfortunately does not solve the problem because by DNI directive a “mission manager’s” authorities are subordinate to the authorities of the several deputies.

18. Dean Acheson, *Present At the Creation* (New York: W.W. Norton & Company, 1969), 28.
