This product is part of the RAND Corporation occasional paper series. RAND occasional papers may include an informed perspective on a timely policy issue, a discussion of new research methodologies, essays, a paper presented at a conference, a conference summary, or a summary of work in progress. All RAND occasional papers undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

OCCASIONAL
PAPER

The Next Steps in Reshaping Intelligence

Gregory F. Treverton

RAND
CORPORATION

This research in the public interest was supported by the RAND Corporation, using discretionary funds made possible by the generosity of RAND's donors and the fees earned on client-funded research.

ISBN: 0-8330-3857-5

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published 2005 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

The shock of September 11, 2001, and the tenacity of the national commission that investigated the disaster produced what decades of previous blue-ribbon panels could not—the beginnings of a real reshaping of U.S. intelligence, in the form of December 2004 legislation. Yet the emphasis is on "beginnings." The law created new boxes on the organization chart and moved others. However, the authorities with which it endowed the main box, the Director of National Intelligence (DNI), are ambiguous. The challenge for the DNI, John Negroponte, is to turn that hunting license into real authority.

Beyond that, the next steps in reshaping U.S. intelligence involve how the Intelligence Community does its business more so than how it is organized. After discussing what has been done so far, and why, this paper lays out that agenda of next steps. It draws on a number of projects for various intelligence agencies, as well as additional research.

This occasional paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by the generosity of RAND's donors and by the fees earned on client-funded research.

This research was conducted within the Intelligence Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the unified commands, the defense agencies, the Department of the Navy, the Marine Corps, the U.S. Coast Guard, the U.S. Intelligence Community, allied foreign governments, and foundations. For more information on RAND's Intelligence Policy Center, contact the Director, John Parachini. He can be reached by email at john_parachini@rand.org; by phone at (703) 413-1100; or by mail at RAND Corporation, 1200 South Hayes Street, Arlington, VA 22202-5050. More information about RAND is available at www.rand.org.

Contents

Summary

The bill signed by the President in December 2004 could serve as the beginning of a real reshaping of U.S. intelligence, but it is hardly the end. Under the shadow of September 11, 2001, it did what could not be done before—create a Director of National Intelligence (DNI) in charge of the 15 U.S. intelligence agencies. Yet the law gives the DNI, John Negroponte, a hunting license more than a full mandate. As the commission investigating U.S. intelligence on weapons of mass destruction (WMD) put it, he has "broad responsibilities but only ambiguous authorities."

The law reshaped how U.S. intelligence is organized; the next steps are transforming how it does its business—matters much more of organizational culture than of an organization chart. Those next steps are:

- Building capacity to manage
- Shaping intelligence by mission or issue, not collection source or agency
- Improving analysis
- Taking advantage of a very different workforce
- Targeting collection.

Finally, and ultimately most important, the intelligence culture of secrecy and "need to know" is dangerously out of date. That culture is designed to protect information, not share it, which ultimately frustrates almost all reform ideas and efforts. Analysis of terrorist threats, for instance, would be improved by consulting people who have *no* "need to know" but bring a different perspective and might see patterns the ostensible experts do not.

Building Capacity to Manage

In principle, the DNI has broad programmatic authority to develop the National Intelligence Program (NIP) and personnel policy for civilian employees in all the agencies. In that sense, the DNI's authority over the nation's intelligence budget is roughly comparable to that of the Secretary of Defense over total defense spending. The limitations on DNI authority are more apparent at the level of *execution*—for instance, restrictions on moving more than a hundred people to any particular new joint intelligence center or on reprogramming more than 5 percent of any agency's budget.

The challenge for the DNI only begins with formal authority. As the capabilities of "national" collection systems in the NIP have improved, they have become increasingly important to warfighters for tactical purposes, and thus the distinction between "strategic" and "tactical" has blurred. As a result, intelligence and the Pentagon share assets and compete over whose needs are more important, especially because supporting warfighters is an open-ended mission: More is always better. The competition also risks duplication, since the military seeks intelligence systems integral to operational units, ones it can count on. The challenge for the DNI, working with the Secretary of Defense, will be to provide some strategic framework for the argument over needs and thus to reduce the risk of needless duplication.

The starting point is beginning to build the analytic clout to fashion an intelligence program and budget that will be compelling both to internal administration decisionmakers and to Congress. The previous Community Management Staff (CMS)—which the law transferred to the DNI, along with the National Intelligence Council (NIC)—is nowhere near up to the task. Its budget function was largely confined to lobbying for programs and to a "bean-counting" review; in conflicts with the Pentagon, it almost always lost.

Relations between the DNI and the Central Intelligence Agency (CIA) Director will be complicated. Director Negroponte seemed to win the early rounds, with the President indicating that he, not the CIA Director, would deliver what had been the CIA's crown jewel, the President's Daily Brief (PDB). Yet the DNI has two jobs—managing the Intelligence Community and serving as the principal intelligence advisor to the President—and balancing the two will be no easy feat. A DNI who tilts the balance between managing and advising too far toward the former would risk losing the credibility to manage. Conversely, tilting it too far toward the latter would risk losing the time to manage.

Shaping Intelligence by Mission, Not Collection Source or Agency

Cold War intelligence was organized, on the collection side, around sources—signals (SIGINT), imagery (IMINT), and espionage (human intelligence, or HUMINT)—and, on the analytic side, around agencies, such as the CIA or the Defense Intelligence Agency (DIA). The most sweeping change in the law created national intelligence centers under the authority of the DNI, which are organized around issues or missions. The centers, with the National Counterterrorism Center (NCTC) as the prototype, would both deploy and use the information, technology, and staff resources of the existing agencies—the CIA, DIA, National Security Agency, and others. The centers would be intelligence's versions of the military's "unified commands," looking to the agencies to acquire the technological systems, train the people, and execute the operations planned by the national intelligence centers.

The December bill licenses the creation of centers but has little to say about any center other than NCTC. The DNI will have to decide which ones to create and, more important, begin to fashion the infrastructure of both technology and people to enable them and change the culture to accommodate them. The existing agencies will resist becoming mere "force providers," not "doers," and will argue, with some reason, that the centers will be consumed by the very hottest current issues.

Improving Analysis

The WMD Commission was direct, and damning, about intelligence before the Iraq war: "This failure was in large part the result of analytical shortcomings; intelligence analysts were too wedded to their assumptions about Saddam's intentions." The need to reshape analysis is dramatic. Current and future threats to the United States are global and adaptive, blurring distinctions between crime, terrorism, and war. State threats come with a shape and "story," one shared by intelligence and policy, but terrorist threats do not. Most important, given the asymmetric nature of the threat, future analysis becomes net assessment, where understanding "blue"—what the United States is doing—is as critical as understanding "red"—U.S. foes. But that idea runs directly against powerful norms in U.S. foreign intelligence—that is, "Thou shalt not assess America or Americans."

Today's analysis is dominated by the urgency of the immediate. The crown jewel analysis, the PDB, is jokingly referred to as "CNN plus secrets." In fact, intelligence needs to provide both current reporting and deeper understanding. In solving puzzles about the Soviet Union, analysts worked alone or in small groups, as parts of hierarchies. In trying to understand terrorism, analysts need to be part of larger virtual networks, across specialties and agencies. Moving toward a center-based organization will facilitate those networks.

But the centers will need to be accompanied by a wide range of experiments and innovations in analysis—to reach out beyond secrets; to make much wider use of method and technology for aggregating expert views to searching, data mining, and pattern recognition; and to search data for the out of the ordinary, not just for confirming evidence. The groups inside intelligence that are thinking beyond the immediate—the NIC, for instance, or the CIA's Strategic Assessments Group—need to be reinforced.

Taking Advantage of a Very Different Workforce

All the intelligence agencies have grown dramatically since September 11, 2001, and this growth has provided wonderful opportunity. The young recruits are fearless and computer savvy. They will not stand for the information environments—compartmented, slow, and source driven—that current intelligence provides. Nor will they long be satisfied with work beats that amount to, as one new recruit put it, "a few square miles of Iraq."

The Intelligence Community will not attract, or will soon lose, these young people if it does not accommodate to how they think and learn. At the front end of the personnel cycle, intelligence might take advantage of demographics and build "gray-green" teams like the best Wall Street firms, combining savvy veterans with fearless newcomers. Lateral entry has been rare, particularly given the demands of security clearance, and a large percentage of those who have joined have stayed for an entire career. That will not be true into the future, though. Many young professionals, seeking challenges, will want to move on, perhaps returning later, pursuing what might be called "portfolio" careers, combining experiences in different sectors. At the senior ranks, too, intelligence needs to open up, inviting in economists, scientists, and other senior professionals it could not hope to retain for a career but might call upon for stints of several years.

The influx can also be an opportunity to build real "jointness" in what is called the Intelligence "Community" but in reality is not. In that sense, training ought to emulate the military in being joint and integral to careers. At present, intelligence is very far from that vision. For the most part, training is discretionary and individual, not required and strategic. Too often the best intelligence officers are deterred from training by the imperative not to "leave the flagpole." And intelligence agencies do not have the slack in their officer ranks to permit officers to routinely depart for several months or even a year. The newly created National Intelligence University can be the capstone and symbol of jointness in training.

Targeting Collection

In the words of the WMD Commission: "The intelligence failure in Iraq did not begin with faulty analysis. It began with a sweeping collection failure." Every blue-ribbon panel calls for improving America's espionage, or HUMINT. The call is worthy, but expectations have to be reasonable. Beyond HUMINT, much of the U.S. collection architecture, such as satellites for IMINT and eavesdropping, is pretty well understood by would-be adversaries. Those adversaries routinely camouflage sensitive activities when they know satellites are overhead. As a result, U.S. intelligence produces too many data and too little information: New technical collection systems, especially for imagery, threaten to overwhelm processing.

Thus, the long-term challenge for U.S. intelligence is to move away from passive surveillance techniques toward more directed collection and to shorten the cycle of innovation so as to be less predictable for would-be targets. For espionage, that means making much more use of America's ethnic diversity and moving spying out of official cover. That will require, however, both money and the least American of traits, patience. On the technical side, innovations may remain secret but, as in Silicon Valley, not for long; therefore, intelligence will have to adapt faster than its targets if it is to stay ahead. For signals, adapting means finding new ways to get very close to its targets; for imagery, it means more use of smaller satellites, or drones, or stealth technology. It also means using new parts of the spectrum, like hyperspectral imagery, to identify effluents from buildings or factories, as well as a range of technologies in what is called MASINT, or measurement and signature intelligence.

Pushing innovation and making better choices across the collection stovepipes is the chief rationale for having a DNI in the first place. The DNI can begin to develop the analytic capacity to make trade-offs across them: How do ground stations compare with satellites for particular SIGINT missions? Can HUMINT do a mission more cheaply? The existing Collection Concepts Development Center, which assesses collection against particular targets, across the stovepipes, is one place to start. The WMD Commission suggests that the DNI create an "integrated collection enterprise" for the Intelligence Community to provide for coordination across the entire cycle—from planning new systems, to developing strategies for deploying existing systems against priority targets, to processing and exploiting information that is produced.

Acknowledgments

I appreciate, in particular, the very helpful reviews given by Loch Johnson and Leslie Lewis. However, neither they nor any of my colleagues in projects related to this paper should be held responsible for any shortcomings that might remain; I alone am responsible for any errors.

Abbreviations

CD	Counterintelligence Division (FBI)
CENTCOM	Central Command
CIA	Central Intelligence Agency
CMS	Community Management Staff
CTC	Counterterrorism Center (CIA)
CTD	Counterterrorism Division (FBI)
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
FBI	Federal Bureau of Investigation
GERP	Global Expertise Resources Program
HUMINT	human intelligence
IMINT	imagery intelligence
INR	Bureau of Intelligence and Research (Department of State)
JMIP	Joint Military Intelligence Program
MI5	Security Service (United Kingdom)
NCTC	National Counterterrorism Center
NGA	National Geospatial-Intelligence Agency
NIC	National Intelligence Council
NIO	national intelligence officer
NIP	National Intelligence Program
NOC	nonofficial cover
NRO	National Reconnaissance Office
NSA	National Security Agency
PDB	President's Daily Brief
SIGINT	signals intelligence
STEP	Science and Technology Experts Program

TIARA	Tactical Intelligence and Related Activities
TTIC	Terrorist Threat Integration Center
WMD	weapons of mass destruction

CHAPTER ONE

Introduction

The bill signed by the President in December 2004 could serve as the beginning of a real reshaping of U.S. intelligence, but it is hardly the end. At last, someone is in charge of American intelligence. To be sure, the reform skeptics, especially in the House Armed Services Committee, snatched a near victory at the eleventh hour. The new Director of National Intelligence (DNI) will not have a free hand to dramatically reshape American intelligence, for instance, by collapsing all the intelligence collectors into a single agency. In the words of the WMD Commission, the law gives the DNI "broad responsibilities but only ambiguous authorities."[1] It is more a hunting license than a full mandate.

Yet the idea of creating a DNI always was going to be just a beginning. In pushing that measure, the 9/11 Commission did an impressive job of selling a good idea that had only a little something to do with the events of September 11.[2] What the 9/11 Commission documents so vividly were operational failures, too little sharing of information, and insufficient attention to the counterterrorism mission, especially by the Federal Bureau of Investigation (FBI).[3] The creation of a DNI is only indirectly related to those failings. In the short run, reaction to the events of September 11 has impelled better day-to-day cooperation among the different elements of the Intelligence Community. In the long run, having someone in charge should make for better cooperation between the FBI and the Central Intelligence Agency (CIA). But as two generations of Secretaries of Defense have found in pressing for more "jointness" among the military services, the task is long and arduous.

A DNI is more directly relevant to the failure to correctly assess Iraqi WMD in the run-up to the 2003 Iraq war, a failure rooted in weak collection against a secretive foe, strong presumptions, and weak checking of what sources did exist. Yet, in this case as in most other intelligence "failures," the key villain was mind-set or presumption—in this case, that Saddam *must* have some WMD, a belief so widely shared, including by those who thought going to war was a bad idea, as to be almost impregnable. When presumptions are so strongly held,

[1] Formally, *Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington, D.C., 2005. Online at http://www.fas.org/irp/offdocs/wmdcomm.html (as of September 2005). Hereafter referred to as "WMD Commission" and "WMD Commission Report."

[2] Formally, the National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, Washington, D.C., 2004. Available online at http://www.9-11commission.gov/. Hereafter referred to as "9/11 Commission" and "9/11 Commission Report." The specific recommendations are summarized in the executive summary and spelled out in more detail in Chapter 13, "How to Do It? A Different Way of Organizing the Government."

[3] This assessment looks forward, not backward, but much of that raggedness was not mere bureaucratic rivalry or protecting turf; it happened because the American people, fearing the misdeeds of concentrated police and intelligence power, had separated the two. We did not want the CIA and the FBI to cooperate *too* well. See, for instance, Gregory F. Treverton "Intelligence, Law Enforcement, and Homeland Security," The Century Foundation, August 2002. Online at http://www.homelandsec.org/publications.asp?pubid=278 (as of September 2005).

it is hard to imagine innovations in intelligence that could shake them; surely, organizational fixes are not likely to do so.

As a result, the real agenda of intelligence reform remains ahead of us. The 2004 bill increases the power of the DNI to allocate Intelligence Community resources, but by how much remains to be seen. Real reforms are much more matters of organizational culture than of an organization chart. The first of these will be actually implementing the recommendation to organize intelligence around issues or threats, not collection sources or agencies. The second is improving intelligence analysis, which was identified by both commissions as the heart of the problem. The 9/11 Commission's recommendations did not really touch that issue, but the WMD Commission made numerous and creative suggestions.

Third on the agenda is dealing with a very changed intelligence workforce, which presents both challenges and opportunities. Fourth is pursuing new, more targeted collection and in the process doing something about the information overload, even from secret systems, that threatens to overwhelm analysts, not to mention policymakers. Finally, and ultimately most important, the intelligence culture of secrecy and "need to know" is dangerously out of date. That culture ultimately frustrates almost all reform ideas; it was discussed by both panels but addressed in the bill only indirectly, through information sharing. In short, creating the DNI and a new organizational superstructure for the Intelligence Community is a necessary but not sufficient step to bring about real reform in how the community does its business.

This paper first summarizes what the 2004 bill does and does not do, then lays out the rationale for the main recommendations from the 9/11 panel that the bill embodied. In conclusion, it turns to the next steps in the agenda of reshaping U.S. intelligence.

CHAPTER TWO

Where Reform Stands

In an unusual move for a blue-ribbon panel, the 9/11 Commission took the reshaping of American intelligence into new territory. Its report was dramatic, and it made a number of recommendations primarily to reshape the organization of U.S. intelligence but also to begin to change the way the Intelligence Community does its business. Still more unusually for a blue-ribbon panel, the commission did not report and then disappear. Rather, it stayed around, hectoring both Congress and the administration to actually make something happen. The 9/11 victims' families added political clout to the commission; they were not about to be ignored. Were it not for them, the commission may not have been established in the first place; once established, the families fought hard for public hearings and for access to President Bush by the commission, and they helped with the lobbying after the report was out. The result was the December 2004 bill creating a DNI, with veteran diplomat John Negroponte appointed the first director in February 2005, reportedly after a number of other candidates had either turned the job down or taken themselves out of the running.

The 9/11 Commission's Recommendations

The 9/11 Commission made six broad proposals affecting intelligence, which serve as a good benchmark for assessing what has been done so far. The WMD Commission, which reported after the bill had been enacted, extended the agenda of reform. Neither commission called for a domestic intelligence service separate from the FBI. Both commissions, and especially the 9/11 Commission, underscored the enormous challenge—one that is the work of years, not weeks or months—of the need not only to create the technical infrastructure to better share intelligence but also to rethink the web of "need to know" and other security requirements that frustrate sharing. The 9/11 Commission's principal recommendations were to

- Create the position of DNI, located in the White House, possessing what the existing Director of Central Intelligence (DCI) did *not* have: real authority over the budgets of the 15 U.S. intelligence agencies
- Institute a National Counterterrorism Center (NCTC) reporting to the DNI, responsible for joint operational planning *and* joint intelligence
- Establish national intelligence centers, organized around discrete issues on the model of NCTC, under the authority of the DNI
- Make the CIA Director a position separate from the DNI and charge him or her primarily with building a better espionage capacity for the nation

- Set focal points for oversight in both the House and the Senate, for both intelligence and homeland security, in place of the 88 committees and subcommittees of Congress before which Department of Homeland Security (DHS) officials now appear
- Rethink the web of "need to know" and other security procedures that frustrate not just sharing intelligence but intelligence work as a whole
- *Not* create a separate domestic intelligence service, on the model of the British MI5; instead, the FBI should move forward with changing its mission from pure law enforcement to terrorism prevention and building a Directorate of Intelligence within the existing FBI.

The first four recommendations were embodied, albeit in differing degrees, in the December 2004 bill. The measure that got the most media attention—creating a DNI—is the most familiar. The most far-reaching recommendation, however, was the commission's proposal to foster coordination by emulating the military in separating the "organize, train, and equip" function from the actual deployment of intelligence personnel. The existing agencies—CIA, FBI, Defense Intelligence Agency (DIA), and National Security Agency (NSA)—would, like the military services, be responsible for *building* the intelligence forces, but those forces would be *used* by the new national intelligence centers, which would be shaped by issue or function, not as now by organization or collection source.

Those centers would be intelligence's equivalent of the military's unified commands. In Iraq, for instance, it was Central Command (CENTCOM) that conducted the war; the troops were provided by the military services, which executed operations under CENTCOM's direction. By analogy, NCTC would be the "unified command" in the war on terrorism, responsible for intelligence analysis and planning operations; the CIA and other agencies would provide the analysts and other personnel and would conduct the required operations—for instance, intelligence gathering. Issue-oriented centers have existed in the intelligence community since the mid-1980s. In form, these centers, like the preexisting Counterterrorism Center (CTC), worked for the DCI; however, in reality, they were dominated by the CIA. The 2004 legislation would move them to the DNI and, in principle, make them more central as focal points for intelligence and operations.

Predictably, the sticking point in the final congressional negotiations was the exact power of the DNI over the intelligence operations located in the Department of Defense (DoD), especially the big technical collectors—NSA, the National Geospatial-Intelligence Agency (NGA), and the National Reconnaissance Office (NRO). Those agencies are responsible for the bulk of the national intelligence budget, and no Secretary of Defense has been eager to cede authority over them to the DCI or to the new DNI. By all accounts, Secretary Donald Rumsfeld was no exception. The Senate passed a bill very much along the lines of the 9/11 Commission recommendations, but the House version, while it created a DNI, endowed that position with less authority than the Senate bill did. In conference, the House achieved many of its objectives.[1] Table 1 summarizes the key issues of contention surrounding the bill with regard to the DNI's authority.

[1] The conference report (on S. 2845), and thus the text of the final bill, is available at http://www.fas.org/irp/congress/2004_rpt/h108-796.html (as of September 2005).

Table 1
The Shaping of the Director of National Intelligence's Authority

Issue	Senate Bill	House Bill	Final Bill
Declassification of budget intelligence top line	Declassify budget top line	Retain classified budget top line	Retain classified budget top line
Budget execution	Intelligence funds do not flow through DoD to intelligence agencies	Intelligence funds flow through DoD to intelligence agencies	Intelligence funds flow through DoD to intelligence agencies
Chain-of-command protection	No chain-of-command protection	No need for chain-of-command provision	Specific provision requiring that implementation "respect and not abrogate" existing military chain-of-command statutes
Budget reprogramming	DNI can reprogram unlimited amount of funds without approval of department or agency heads	DNI unilateral reprogram authority capped at 5% of department budgets	DNI unilateral reprogram authority capped at 5% of department budgets
Personnel transfers	DNI can transfer unlimited number of personnel without the approval of department or agency heads	No unilateral personnel transfer authority	DNI unilateral transfer authority is limited to 100 personnel for each new national intelligence center created
Personnel management	DNI can prescribe personnel policies and requirements for all personnel within the intelligence community, including military personnel	DNI personnel policy authorities limited to civilian employees	DNI personnel policy authorities limited to civilian employees
DNI control over military programs	Gives DNI primary control over all programs of NSA, NRO, and NGA, including nonnational military programs (e.g., the Joint Military Intelligence Program [JMIP])	Excludes from DNI primary control over all military intelligence programs within JMIP	Excludes from DNI primary control over all military intelligence programs within JMIP

The most important of these eleventh-hour negotiations were the limits on the DNI's key powers over moving money and people. It will take some time with the new DNI in place to know just how important those limitations will be. In principle, DNIs will have considerable programmatic authority: They will develop the National Intelligence Program (NIP) and broad personnel policy for civilians in all the agencies. In that sense, the DNI's authority over the nation's intelligence budget is roughly comparable to that of the Secretary of Defense over total defense spending. The limitations on DNI authority are more apparent at the level of *execution*—for instance, the restriction on moving more than a hundred people to any particular new joint intelligence center. Beyond the hundred, the DNI will, like the DCI before him, have to bargain with the other agency heads. The 5 percent limit also applies to the DNI's authority to *reprogram* budgeted money without congressional approval. To be sure, 5 percent of a big agency budget is a lot of money, especially in the context of the DNI's programming authority.[2] Still, the task for Director Negroponte will be to convert these ambiguous powers into real authority.

[2] In fact, the law restricts the DNI from transferring more than 5 percent of the agency's budget or $150 million, whichever is smaller, from one agency in one year.

Assessing the Main Provisions

The first three recommendations embodied in the December bill are the heart of the new approach, seeking coordination, or "jointness," at two levels: (1) the strategic, by breaking down the "stovepipes" that now make the separate agencies, especially the big collecting agencies, baronies in their own right, and (2) the day-to-day, by using the national intelligence centers to improve the operational management of intelligence. The first three recommendations formed a cluster, one that cannot easily be disentangled, and have an either-or quality to them, so half-measures in implementation could wind up being worse than doing nothing at all.

Create a Director of National Intelligence

The DNI is charged with overseeing national intelligence centers on specific subjects of interest across the U.S. government, managing the NIP, and overseeing the agencies that contribute to the NIP. The logic of the idea was to give the DNI what the post of DCI lacked: authority over budgets for the intelligence agencies other than the CIA, over the hiring and firing of senior leaders, and over setting standards for the Intelligence Community's personnel and infrastructure.

The DNI replaced the DCI. The position will be confirmed by the Senate, as was Negroponte, and the DNI will testify before Congress. The 9/11 Commission proposed to embody interagency cooperation by giving the DNI three deputies, each of whom would also have had a second agency responsibility: foreign intelligence (the CIA Director), defense intelligence (the Under Secretary of Defense for Intelligence), and homeland intelligence (the FBI Executive Assistant Director for Intelligence or the Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection). The December bill scrapped that arrangement, calling instead for a Principal Deputy Director and up to four other deputies with portfolios assigned by the DNI.[3] Appointing a military person—Lt Gen Michael Hayden, Director of NSA—as Principal Deputy DNI was more than a nod to the Pentagon's concerns that the creation of the DNI might diminish the military's leverage over the major collectors.

DoD's more strictly tactical intelligence programs (dubbed Tactical Intelligence and Related Activities, or TIARA), which serve commands or field commanders, were always slated to remain the Pentagon's responsibility. The Senate bill proposed to give the DNI authority over the Joint Military Intelligence Program (JMIP), a set of tactical joint intelligence activities, some of which came from TIARA and some of which were performed by NSA or by NGA's predecessor organizations. The final bill authorizes the DNI to work with the Secretary of Defense in preparing both TIARA and JMIP budgets, which together total less than a quarter of the total intelligence budget.

Here, as in other areas, the real challenge for the DNI only begins with formal authority. As the capabilities of "national" collection systems in the NIP have improved, they have become increasingly important to warfighters for tactical purposes, and thus the distinc-

[3] This provision echoed the blue-ribbon intelligence panels of the 1990s. For instance, the Aspin-Brown Commission—formally, the Commission on the Roles and Capabilities of the United States Intelligence Community—had called for three assistant DCIs, one each for analysis, collection, and management. Congress later approved that idea. The commission's report is *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, Washington, D.C., 1996. Online at http://www.access.gpo.gov/int/report.html (as of September 2005).

tion between "strategic" and "tactical" has blurred.[4] As a result, civilian policymakers and military warfighters share intelligence assets more and more, and with that sharing, the competition over whose needs are more important intensifies, all the more so because supporting warfighters is an open-ended mission: More is always better. The risk of duplication also grows as the military seeks intelligence systems integral to operational units, ones it can count on. The challenge for the DNI, working with the Secretary of Defense, will be to provide some strategic framework for the argument over needs and thus to reduce the risk of needless duplication.

Several analytic agencies will be important parts of the DNI's "troops" but will also serve particular departments as their in-house analytic cadres, so some creative compromise over authority probably always was going to be required for those agencies. The State Department's Bureau of Intelligence and Research (INR), for instance, numbers only several hundred but often carries weight beyond its size in interagency deliberations. Secretaries of State, however, are bound to regard the INR as *their* intelligence agency. The Secretary of Defense and the Chairman of the Joint Chiefs of Staff are likely to view the DIA in a similar way.

The law gave the DNI the authority to appoint the CIA Director. For all the other intelligence agency heads, save one, the DNI was given a veto through the requirement that he or she concur in the appointment made by the department head (Defense, State, Treasury, etc.) for whom the intelligence agency works. The exception is the directorship of the DIA, for which the law gave the DNI a mandate only to be consulted.

Creating a DNI is hardly a new idea but rather a hardy perennial.[5] In one assessment of 31 studies of or proposals for reforming intelligence between 1948 and 2002, the top three recurring themes were to expand the DCI's authority, create a DNI, and give the DCI more tools to manage the Intelligence Community.[6]

Whatever the connection or lack thereof to the September 11 failure, the need for better strategic management of the Intelligence Community is a pressing one. In the WMD Commission's words, the community is "fragmented, loosely managed, and poorly coordinated."[7] On the collection side, U.S. intelligence's legacy from the Cold War is an organization of collection sources, or "stovepipes," with NSA for signals intelligence (SIGINT); the CIA for espionage, or "human intelligence" (HUMINT); and NGA for imagery intelligence (IMINT). That model was, perhaps, not a bad way to organize intelligence during the Cold War; in effect, all the information gatherers were asked what they could contribute to solving the overarching puzzle of Soviet behavior.

However, the stovepipe model is not the right way to organize U.S. intelligence today, with the many threats, not one; torrents of information, although of widely varying quality; and many customers. Given hard problems and arcane technology, plus a division of

[4] This transformation is discussed at length in Chapter 4 of Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, Cambridge, UK: Cambridge University Press, 2001.

[5] See Alfred Cumming, *The Position of Director of National Intelligence: Issues for Congress*, Washington, D.C.: Congressional Research Service, July 29, 2004. Online at http://www.fas.org/irp/crs/RL32506.pdf (as of September 2005).

[6] Todd Stiefler, *Intelligence Restructuring: Patterns and Pitfalls*, unpublished RAND Corporation research. See also Richard A. Best, Jr., *Proposals for Intelligence Reorganization, 1949–2004*, Washington, D.C.: Congressional Research Service, July 29, 2004. Online at http://www.fas.org/irp/crs/RL32500.pdf (as of September 2005).

[7] WMD Commission Report, p. 5.

labor that gave control of their purse strings to the Pentagon but ostensible oversight to the DCI, the stovepipe managers have had considerable autonomy. Moreover, once the retrieval times for gathering the information became short enough to make that information useful to battlefield commanders, the Pentagon incorporated the stovepipes into real operational decisionmaking that has made possible pinpoint targeting of adversaries from afar. But strategic and tactical were blurred, and it became still harder for the DCI to control how technical resources were allocated.

The case for ending the long mismatch between the responsibility of DCIs and their authority is a strong one. Creating a DNI would accomplish that while serving as a counterbalance to the recent tendency of military consumers to dominate U.S. intelligence. The question that remains to be seen is whether the December bill really ends that mismatch and creates that counterbalance. DNIs will have veto authority over the appointments of the main agency heads, and they will have budgetary initiative and some authority over execution, as indicated in Table 1.

A lot of the initiative, however, will still rest with the Pentagon, and the DNI will have to move fast to create troops, build authority, and work out arrangements with the Secretary and Under Secretary of Defense. The law provided for the transfer of the National Intelligence Council (NIC) to the DNI, along with the NIC's counterpart for the business of the Intelligence Community, the Community Management Staff (CMS). As it was, however, CMS was nowhere near up to the task of helping DNIs actually manage the community; recognizing that, the law provides for 500 new official positions for the DNI, plus 150 to be transferred from other agencies. CMS's budget function was largely confined to lobbying for programs and to a "bean-counting" review; in conflicts with the Pentagon, it almost always lost. It will take time to build the analytic clout to fashion an intelligence program and budget that will be compelling both to internal administration decisionmakers and to Congress.

To enhance the clout of the new position, the 9/11 Commission recommended that the DNI be located in the Executive Office of the President. The December bill, however, directly stipulated that the DNI would *not* be in the Executive Office of the President. A common perception in political Washington is that location bespeaks power and thus betrays perspective. At one extreme, a DNI housed at CIA headquarters would make it clear that the CIA Director was a subordinate but would risk that the DNI would become a captive of the CIA, viewed as such today. At the other extreme, a DNI housed with only a few subordinates at the Old Executive Office Building, next to the White House, would be close to power but risk looking like drug czars in previous administrations—long on title but short on troops. The present plan is neither; the DNI and his core staff will be housed, temporarily, in DIA facilities at Bolling Air Force Base in southwest Washington.

The 9/11 Commission and the Senate bill endorsed making the top lines of the U.S. intelligence budget public, a move that is long overdue. Detailed numbers would have remained secret, but the overall budget allocations and the apportionment among agencies could have been safely disclosed without harm to intelligence's "sources and methods." Indeed, keeping them classified when they are bandied about in the press only makes it look like the government has something to hide. It is a shame that America now lags Britain, the land of official secrets, which makes its top-line budget numbers known. Unfortunately, the failure of the December bill to make the top-line number public has only compounded that shame.[8]

The main reason there was no DNI despite nearly 50 years of calls for one is that none of the most critical officials wanted the change.[9] For their part, DCIs have not wanted to trade their CIA troops for the uncertain prospects of being an intelligence overlord. Secretaries of Defense—and their congressional overseers—had been loath to lose control of critical information-gathering agencies. When, in the 1970s, the White House proposed to give control of the big technical collectors to the DCI, Secretary of Defense Rumsfeld (in his first stint as Secretary, in the Ford administration) is said to have replied: "If they're in my budgets, I'll run them."[10] The growing importance of those big intelligence collectors in the scheme of military transformation, if anything, probably increased the defense establishment's opposition to giving a DNI control. It took the shock of September 11 and the pull of the victims' families, plus the artful connecting by the 9/11 Commission of that failure with the need for a DNI, plus continued lobbying by the commission members to make the December bill a reality.

Create a National Counterterrorism Center

This new office will be responsible for both joint operational planning and joint intelligence.[11] The Terrorist Threat Integration Center (TTIC), created in 2003, became NCTC, or at least half of it. It became, in effect, NCTC's intelligence analyst. The bill gave NCTC the authority to work out exactly what the planning task, labeled "strategic operational planning," would entail and how it would work. NCTC, like TTIC before it, is to absorb much of the analytic talent now residing in the CIA's CTC and in DIA. TTIC was created to "connect the dots" of intelligence, both foreign and domestic, and warn of terrorist threats to the homeland. In effect, TTIC became, on the intelligence side, the center of a confederation, with several hundred officials from the CIA's CTC and from the FBI's Counterterrorism Division (CTD) located at NCTC headquarters, Liberty Crossing, in Tysons Corner, Virginia, not far from CIA headquarters.

On the strategic operational planning side, NCTC draws on a limited inheritance. The CTC, for instance, from the start was located with the CIA's clandestine operators, the Directorate of Operations, and was more engaged in providing operational support to intelligence operations abroad than it was in pure analysis. NCTC, however, as framed by the bill, would neither execute operations—those would be left to the agencies—nor make policy —which would be left to the President and the National Security Council. It would assign

[8] As elsewhere in life, the "devil is in the details," and, intriguingly, the purpose of the 9/11 Commission and Senate legislators was only partly public accountability. Part of their purpose was procedural: If the top-line budget were public, it could be appropriated directly and publicly to the DNI. The DNI would be in visible charge. If, however, the top line remained secret—as it did in the final bill—the budget would still have to be "laundered" through the Pentagon, and even if the DNIs had had full control in principle (which the final bill did not give them), their control still might have been diluted by the pass-through in the Pentagon.

[9] President Truman and his confidants wanted a more powerful DCI in the late 1940s but retreated in the face of Pentagon and State Department opposition, especially so because the administration's eyes were fixed on the main prize, a more centralized Pentagon. See Loch K. Johnson, "A Centralized Intelligence System: Truman's Dream Deferred," *American Intelligence Journal*, forthcoming.

[10] Walter Pincus, "Military Espionage Cuts Eyed," *Washington Post*, March 17, 1995, p. A1.

[11] The model is explicitly that of military joint staffs, and the center will play the roles of both J-2 (intelligence) and J-3 (operational planning).

responsibilities for operations to lead agencies but not direct the execution of those operations.

The head of NCTC is to be appointed by the President and confirmed by the Senate. The DNI will oversee the center's operations and budget, and the NCTC Director will report to the DNI on intelligence and intelligence operations. However, with regard to counterterrorism operations other than those in intelligence, the NCTC Director will report to the President. That dual reporting is probably necessary if NCTC is to play a real role in planning the government's counterterrorism operations, including those undertaken by the Pentagon. It does, however, run the risk of further weakening the DNI position by dividing the loyalty of a principal subordinate.

On the positive side, the conception of NCTC is rooted in the presumption that counterterrorism is intelligence rich and thus that planning needs to be intelligence driven. In general, the government achieves interagency coordination in one of two ways: designating a lead agency or passing the coordinating responsibility to the White House (e.g., the National Security Council). If an agency leads, it then constructs its own means of achieving interagency coordination. The CTC at the CIA, for example, recruits liaison officers from throughout the intelligence community. The military's unified CENTCOM has its own interagency intelligence center, recruiting liaison officers from all the agencies from which it might need help. The FBI has joint terrorism task forces in 84 locations to coordinate the activities of other agencies when action is required.

The December bill seems to indicate a mix of coordination by NCTC and by the White House, presumably the National Security Council but perhaps the Homeland Security Council.[12] NCTC will coordinate planning but will then turn execution over to lead agencies. The operational coordination presumably would be done by some combination of those lead agencies and the National Security Council. In general, counterterrorism operations tend to range across diplomatic, law enforcement, military, and intelligence instruments, and so pose hard challenges to coordination—and to lead agency coordination in particular.

The first challenge for the NCTC Director and the DNI will be to sort out the turf battle between NCTC (and its predecessor, TTIC) and the CTC. The WMD Commission pointed to this tug-of-war over resources, authorities, and responsibilities, a guerrilla war that has raged since the creation of TTIC. A division of labor might have the CTC concentrate on support to operations, while NCTC focuses on intelligence analysis and planning, and not all competition between the two need be negative. But sorting out the roles of the two will be a first test of whether the DNI and his team are really in charge.

Create National Intelligence Centers

With NCTC as the prototype, creating national intelligence centers under the authority of the DNI and organized around issues was the most sweeping change in the way intelligence does its business proposed by the 9/11 Commission. The centers would both deploy and use the information, technology, and staff resources of the existing agencies—the CIA, DIA, NSA, and others. They would be the "unified commands" looking to the agencies to acquire

[12] The 9/11 Commission suggested that the existing Homeland Security Council be merged into the National Security Council—a recommendation also made in a recent RAND study. Lynn Davis et al., *Coordinating the War on Terrorism*, Santa Monica, Calif.: RAND Corporation, OP-110-RC, 2004. The bill does not do so.

the technological systems, train the people, and execute the operations planned by the national intelligence centers. They would bring together analysts, information collectors, and operations specialists around problems or issues, not collection sources or agencies.

The December bill licenses the creation of national intelligence centers but has little to say about the ones other than NCTC. The 9/11 Commission suggested that the centers be organized around a mix of functional and regional issues—weapons of mass destruction, crime, Russia and Eurasia, and the like. At present, several centers, such as the existing CTC, bring together officers from a number of intelligence agencies. The commission's proposal would intensify these liaisons by making the national intelligence centers the primary means through which the Intelligence Community does its work. Now, the centers are still the creatures of the agencies. In the commission's proposal, the agencies would become their supporters. Ideally, those who use intelligence in this age of terrorism would be drawn toward the centers and would know where to go for one-stop shopping in their areas of interest.[13]

There are several lines of concern about a center-based organization. The first is that no real infrastructure exists to support the concept, in technology or personnel. There is little tradition of intelligence officers moving, and little incentive for them to do so. The technical shortcomings are obvious at NCTC, where analysts' computers are accompanied by a half-dozen "pizza boxes"—different agency information sources that have to be integrated by the analysts.

Also on the capacity-building side, the big analytic agencies resist thinking of themselves as force providers; they regard themselves as the doers. Already, those agencies express concern about "center-itis," the rise of numerous specialized or issue-oriented centers.[14] They tend to think of personnel assigned to those centers as lost to the real work, which happens back home at the agency. Changing that view to regard the real work as done by the centers, with the agencies in a supporting role, would entail a sea change in organizational culture.

Second, the existing agencies will argue that the centers as the primary producers of intelligence would be very much inclined toward focusing on current intelligence and would tend to produce worst-case analyses. Based on the experience of the military's unified commands, those are serious objections, although at this point the analogy between the centers and the military commands begins to break down. The unified commands do tend to have short time horizons and worry about worst cases, for understandable reasons: If war broke out today, they would have to fight it. In a similar way, the centers would be the first ones blamed if crises developed without warning, and their plans would be the first ones exposed if remedies failed. So the bias toward current intelligence and the dramatic over-warning that now afflict all of U.S. intelligence could get worse.

In the end, it is a matter of degree and of countervailing pressures. Already, the bias toward today's hot issues is pervasive. With a changed structure, a DNI would need to make all the surer that there are places, such as the existing NIC or the CIA's Strategic Assessments Group, that lean against the wind and provide at least a little protection from the urgency of the immediate.

[13] See Chapter 7 of Treverton, *Reshaping National Intelligence*, on the need for such a structural reorganization.

[14] That resistance came through loud and clear in interviews throughout the analytic elements of the Intelligence Community in 2004. See Gregory F. Treverton and C. Bryan Gabbard, *Assessing the Tradecraft of Intelligence Analysis*, Santa Monica, Calif.: RAND Corporation, forthcoming. The bias toward current intelligence was even more marked. That bias is a central theme of the WMD Commission Report.

The WMD Commission recommended creating a second center, one mentioned in the bill and adopted by the Bush administration—a National Counter Proliferation Center. That center, however, is to be structured very differently from NCTC. The center will be small and focused on overseeing collection and analysis. Planning and operations will be left to wider interagency groupings.

The WMD Commission also suggested building on the center concept by appointing "mission managers" for priority topics. Those managers, who would work for the DNI, would drive collection and oversee analysis in their areas, and they would serve as a clearinghouse for senior policymakers seeking expertise in that area. Interestingly, this conception is akin to the original notion of national intelligence officers (NIOs) in the early 1970s. Influenced by their experience with a special assistant for Vietnam affairs, DCIs James Schlesinger and William Colby fashioned the NIOs as points for one-stop shopping in their respective areas.[15] The challenge the mission managers will face is the same one NIOs have faced before them: knowing enough about collection sources and technologies to actually have some effect on collection.

Make the CIA Director Separate from the Director of National Intelligence

In the 9/11 Commission's vision, more or less incorporated in the final bill, the CIA Director would be primarily responsible for building a better espionage capacity for the nation. The DCI—now CIA Director, Porter Goss, appointed in 2004—did indeed make that his, almost exclusive, priority. The task would include, in the commission's words:

> transforming the clandestine service by building its human intelligence capabilities; developing a stronger language program, with high standards and sufficient financial incentives; renewing emphasis on recruiting diversity among operations officers so they can blend more easily in foreign cities; ensuring a seamless relationship between human source collection and signals collection at the operational level; and stressing a better balance between unilateral and liaison operations.

No DCI has wanted to surrender direct management of the CIA, fearing that the loss of "troops" would mean a loss of power. The commission recognized that risk but argued that clandestine operations are tactical and require close attention. In any case, if the DNI ran the CIA, that official would be both advocate for CIA funding and administrator of overall intelligence funding—a conflict of interest. It also noted that the law charges the CIA with *foreign* intelligence, while the critical task for the DNI will be coordinating intelligence across the foreign-domestic divide.

It is interesting to note that when the CIA was first created in the 1940s, it was intended to be what its name implied—a central coordinating office. It was not expected to produce much analysis of its own, nor was it expected to conduct clandestine intelligence operations abroad. The State Department's distaste for clandestine operations soon got the CIA involved in operations, and the military's lack of interest or cumbersomeness in developing spy planes and spy satellites got the CIA into the technology business. Soon, it had become not the coordinating agency but another agency needing coordination, and so the conflict of interest between the DCI's roles as CIA Director and overseer of all intelligence

[15] See William Colby, with Peter Forbath, *Honorable Men: My Life in the CIA*, New York: Simon & Schuster, 1978, pp. 352–353.

emerged. That conflict was muted only because the DCI did not have much authority in the overseer role.

More important, having the DNI also run the CIA would create an overwhelming workload, even worse than the one now faced by the DCI. As the 9/11 Commission put it:

> The DCI now has at least three jobs. He is expected to run a particular agency, the CIA. He is expected to manage the loose confederation of agencies that is the intelligence community. He is expected to be the analyst in chief for the government, sifting evidence and directly briefing the President as his principal intelligence adviser.[16]

The 9/11 Commission hoped that a DNI would be able to exercise the third responsibility while really managing the second.

The DNI will still have two jobs, and balancing the two will be no easy feat. A DNI who tilts the balance between managing and advising too far toward the former will risk losing the credibility to manage, but one who tilts it too far toward the latter will risk losing the time to manage. And, to be sure, relations between the DNI and the CIA Director will be complicated. One insider likened the process of working out which CIA and Intelligence Community functions housed at the CIA would stay there and which would go to the DNI to the "partition of India." Will both the DNI and the CIA Director meet the President in the morning with the President's Daily Brief (PDB)? And who will prepare that brief? The new DNI, Negroponte, seemed to win the early rounds, with the President indicating that he, not CIA Director Goss, would deliver what has been the CIA's crown jewel. Eventually, relations between the two might evolve into something like that between the Attorney General and the FBI Director, who, in form, are boss and subordinate but, for some purposes, interact much more like equals.

As the DNI tries to build authority over budgeting and executive hiring decisions and be the President's principal national intelligence officer, he will need the assistance of a dedicated intelligence staff. NCTC, along with the other centers, might effectively serve as such a staff. So might the NIC, whose role is underscored by the bill. The NIC, however, is likely to be stretched by the tension between a newly enhanced role in current intelligence, as overseer in some form of the PDB, and its traditional role as producer of deeper and longer-term intelligence, especially the National Intelligence Estimates.

In one area, paramilitary operations, the 9/11 Commission would have the CIA cede responsibility for directing and executing operations to the military. However, the commission finds the Afghanistan precedent of joint CIA-military teams a good one and suggests that CIA capabilities and people should be integrated into military-directed teams, giving both the CIA and special operations forces the opportunity to do what each does best. But the December bill was silent on this issue, and the CIA and the military decided that both would remain in the paramilitary operations business.

Like other of the 9/11 Commission's major recommendations, this one, too, has a long and hoary history. The arguments for giving control to the military have been, historically, the ones the commission cited: the requisite capabilities are military; the task has not been a continuous priority for the CIA; and it makes no sense for the nation to build two

[16] This language is very much akin to my own in Treverton, *Reshaping National Intelligence for an Age of Information*, p. 235.

parallel capacities. Another concern is that the military was never very agile or discreet, let alone covert. That concern may have diminished, but not disappeared, as the special forces have developed a wide variety of units and types of operations.

Whatever else is occurring, special operations forces and the CIA are being thrust together. That seemed an effective partnership, especially in Afghanistan, and the commission applauds it. It does, though, raise thorny questions of authorization and accountability, ones that are not settled by the commission's recommendation. Operations by the military would give those carrying them out the status of combatants under international law, at least if they were visibly soldiers.

CIA covert actions require a presidential finding, one transferred in secret to the relevant committees of Congress. By contrast, a similar operation conducted by the special forces could be set in motion simply by the chain of command from the President as commander in chief. The difference may be less than meets the eye, however, if findings have become so broad in the war on terror as to cover almost any CIA operation. If so, however, the problem lies with the breadth of the findings.[17] If they are so broad as to cover almost anything, then the finding process has become a sham.

Do *Not* Create a Separate Domestic Intelligence Agency

Both commissions decided, and Congress agreed, that the arguments for creating a separate domestic intelligence service, at this point in time, were not persuasive and that the FBI should be given time and encouragement to build its own intelligence capacity. The WMD Commission did, however, go further than the 9/11 Commission and recommended creating not just a Directorate of Intelligence within the FBI but a National Security Service, incorporating intelligence plus the FBI's CTD and Counterintelligence Division (CD). It feared that even a beefed-up Directorate of Intelligence would lack the ability to task the FBI field offices for information or control the intelligence budget, most of which is spent by the CTD and CD.[18] It envisioned an FBI National Security Service with about the same relationship to the DNI that NSA and NGA will have. In 2005, the FBI did create such a service, and in another example of emerging authority, Negroponte appeared to have a significant say in the appointment of its director.

The argument *for* a separate domestic intelligence agency is twofold.[19] The first is that the FBI is likely to remain—and perhaps should remain—primarily a case-based law enforcement organization. It is good at that. Yet pursuing individual cases the way the FBI does simply will not help build a comprehensive intelligence picture.

Second, abuses of the rights of Americans committed by the FBI in the 1960s and 1970s—especially, the so-called COINTELPRO, aimed at suppressing political dissent—

[17] For instance, existing findings apparently provided authorization for the CIA to fire a missile from a Predator drone over Yemen in November 2002. The attack killed six people, including one American. For a newspaper account, see Walter Pincus, "U.S. Strike Kills Six in Al Qaeda: Missile Fired by Predator Drone; Key Figure in Yemen Among Dead," *Washington Post*, November 5, 2002, p. A1.

[18] See WMD Commission Report, p. 30. In the commission's phrase: "The Directorate of Intelligence may 'task' the field offices to collect against certain requirements … [but] its 'taskings' are really 'askings.'"

[19] These arguments are discussed at more length in Treverton, "Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons," *Intelligence and National Security*, Vol. 18, No. 4, Winter 2003.

arose from mixing domestic intelligence with law enforcement.[20] For similar reasons, Canada took its Royal Canadian Mounted Police out of the domestic intelligence business, replacing it with a separate service, the Canadian Security Intelligence Service. Other states have been successful in creating domestic intelligence bodies that have operated effectively within the constraints of liberal democracy, including Britain (Security Service, MI5), France (Direction de la Surveillance du Territoire), Germany (Bundesamt für Verfassungsschutz), and Australia (Australian Security Intelligence Organisation).[21]

Yet the downside of a separate agency also is apparent. In purely practical terms, it would have all the teething pains of any new agency—pains vividly on view at DHS—and, to boot, would need to duplicate the range of offices and infrastructure of the current FBI. (Those teething pains could, however, also be used as an argument for creating the new agency now rather than waiting, if a separate, new agency were viewed as a good idea in principle.) Moreover, a new agency would hardly be a panacea; in Britain, MI5 and Scotland Yard were for years locked in a turf battle over which agency had primary responsibility for counterterrorism in Britain outside Northern Ireland.

Whether accountability and oversight would be better with a separate service is hard to settle in the abstract. On the one hand, a separate agency, concentrating on intelligence and thus overseen solely by the congressional intelligence committees, might be more accountable than a domestic intelligence function linked to law enforcement. On the other hand, a domestic intelligence service completely independent of case-based law enforcement, and outside the purview of the Justice Department, could raise civil liberties concerns.

In the end, all these arguments probably were trumped by the desire to let the FBI continue on its current track. Bureau leaders have committed to a fundamental change in mission and practice. Terrorism is a matter for both intelligence and law enforcement, and now the "wall" that used to separate the two, including the wall that existed within the FBI, has been all but erased. Officials seeking intelligence can share information with colleagues who are investigating a criminal case. To both commissions, this did not seem the right time to tear apart that incipient cooperation by creating a separate intelligence agency outside the FBI.

[20] See *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate*, 94th Congress, 2nd Session, 1976, Book II, *Intelligence Activities and the Rights of Americans*, and Book III, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans.* For links to these reports, as well as to a rich range of other documents, both historical and contemporary, see www.icdc.com/~paulwolf/cointelpro/cointel.htm (as of September 2005).

[21] See Peter Chalk and William Rosenau, *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*, Santa Monica, Calif.: RAND Corporation, MG-100-RC, 2004.

CHAPTER THREE

Initiatives for the Next Phase of Intelligence Reform

The existing legislation is a beginning. And Director Negroponte, someone not from intelligence but versed in it and, perhaps more important, someone who knows how to make the government work, has begun to use the license of the law to hunt for real authority. Much of his task is implicit in his mandate to break down the stovepipes, asking how best the United States will get the information it needs. The challenges to existing organizational cultures are daunting. This section outlines the most important of them that lie beyond developing centers and mission managers to enable the United States to do its intelligence business around issues or threats, not sources or agencies.

Improve Analysis

Here, the WMD Commission was direct, and damning, about intelligence before the Iraq war: "This failure was in large part the result of analytical shortcomings; intelligence analysts were too wedded to their assumptions about Saddam's intentions."[1] The 9/11 Commission was eloquent about the need for more creativity, but its recommendations did not really touch that topic. Indeed, its main recommendation embodied in the final bill—to organize the analytic part of the Intelligence Community around *issues*, as with NCTC—carries the risk of increasing the urgency of the immediate. Those centers will be consumed by the need to provide the very hottest current intelligence. The law, rather quaintly, makes a gesture toward analysis by requiring "alternative analysis" (defined as "red-teaming" by the law) and mandating that the DNI appoint some person or entity to be the watchdog of integrity and objectivity in the analytic process.[2]

The need to reshape analysis is dramatic. Current and future threats to the United States are global and adaptive, blurring distinctions between crime, terrorism, and war. Analysts of the future will need to think more like homicide detectives, trying to see patterns amid incomplete information. Most important, given the asymmetric nature of the threat, future analysis becomes net assessment, where understanding "blue"—what the United States is doing—is as critical as understanding "red"—U.S. foes. But that idea runs directly

[1] WMD Commission Report, p. 3.

[2] "Red-teaming" is seeking to get inside the heads of adversaries, not asking what we would do if we were them but creatively trying to ask what they might do given their own goals, culture, organization, and the like. Red-teaming is only one technique, albeit an important one, among a family of "what ifs" that go under the label of "alternative analysis." For more information, see Warren Fishbein and Gregory F. Treverton, *Making Sense of Transnational Threats*, Central Intelligence Agency, Kent Center for Analytic Tradecraft, Occasional Papers, Vol. 3, No. 1, October 2004. Online at www.cia.gov/cia/publications/Kent_Papers/pdf/OPV3No1.pdf (as of September 2005).

against powerful norms in U.S. foreign intelligence—that is, "Thou shalt not assess America or Americans."

Traditional intelligence as practiced during the Cold War focused on nation-states; non-state, or "transnational," actors were secondary. Now the priority is reversed, and the principal targets are non-states, like al Qaeda; states are of interest as facilitators of terrorism, willingly or because they lose control of their territory. We know what states are like, even states very different from our own; states are organized in hierarchies. Intelligence and policy officials share a "story" about states. There is much less of a shared story about non-states, which come in many sizes and shapes. Their forms combine network and hierarchy. Understanding them is less bounded, and more outcomes are possible.

Many state targets are, as the Soviet Union was, secretive; information was in short supply, so pride of place went to intelligence's secret sources. Terrorist groups are hardly open, so secrets still matter. But signals about bad people or bad weapons are also there to be ferreted out of the vast "noise" of customs declarations or motor vehicle records, not to mention Web chat rooms. The Soviet Union was not only hierarchical but also ponderous; discontinuities in its behavior were rare. Al Qaeda has shown itself to be patient, but discontinuities in the terrorist threat—new groups or new weapons or new modes of attack—are all too possible.

Critically, Soviet behavior on many issues could safely be assumed to be relatively independent of what we did. As one U.S. Defense Secretary is quoted as saying about Soviet nuclear programs: "when we build up, they build up; when we slow down, they build up." The interaction of what we do and how terrorists respond is much more consequential. After all, terrorism is the tactic of the weak, and so terrorists cannot be understood in isolation from what we are doing to counter them. Even the capabilities of the terrorists turn on us. The September 11 hijackers did not come to their tactic as a preference; rather, they chose it because they had found seams in our defenses.

In the circumstances of the Cold War, the way intelligence was organized made some sense. Both intelligence collection and, only slightly less, intelligence analysis were organized in "stovepipes," the collectors by source and the analysts by function or geographic region. In effect, all were asked what they could contribute to solving the puzzle of Soviet behavior.

In understanding terrorism, by contrast, the need for collaboration is much greater, not just across sources or specialties in federal intelligence agencies but also with foreign partners and with state and local officials. So, too, intelligence's customers were limited during the Cold War, mostly politico-military officials of the federal government. Now, intelligence is called upon to serve a much wider range of consumers, from foreign partners of the United States, which may have access to places and people we do not, to private citizens who own the national infrastructure that terrorists may target—and intelligence is often linked to action on a continuing basis.

During the decade lull between the Cold War and war on terrorism, intelligence's budgets declined and its deep expertise on the Soviet Union dispersed. To be sure, public rhetoric often exaggerates the decline. Both political parties sought a "peace dividend" after the Cold War, but most of that dividend came from defense; for its part, intelligence, which had gone up faster than defense in the 1970s and 1980s, declined more slowly in the 1990s.

And the counterterrorism mission took very little hit; indeed, its budget began to grow rapidly after the bombing of the World Trade Center in 1993.[3]

At the same time as budgets tapered down, intelligence needed new customers and new missions. It found new customers, especially in such economic agencies as the Commerce Department. Those new customers mostly were interested in immediate support, more like staff work than longer-term analysis. With more customers and fewer resources, the intelligence agencies were hard-pressed to keep up with the flood of short-term questions they were being asked. But because intelligence is in the service business, turning away new customers or shucking off old ones is painful. What got squeezed, instead, was the capacity to do deeper analysis.

As many insiders lament, in one form or another: We now do reporting; we used to do analysis. The dominance of question-answering is pervasive, even where it would not be expected. The intelligence agencies of the military services, for instance, report that they spend as much as half their time answering specific, usually short-run, questions, not doing their traditional job of assessing the military capacities of potential U.S. foes. The crown jewel analysis, the PDB, is jokingly referred to as "CNN plus secrets." It *is* very current, often a new piece of secret information, although analysts do add commentary to put that information in context.

In fact, intelligence needs to *both* answer immediate questions and open space for longer-term thinking. Both will require dramatic changes in the way intelligence does its business. Instead of relying heavily on secret sources, intelligence has to reach out to a wider variety of sources. In a former world of secret sources, analysts could be separated from intelligence collectors; in today's world of the Web, analysts are also their own collectors. In the world of secrets, analysts were mostly passive users of what information was delivered to their computer screens; now they need to actively search and question data, something that comes naturally to the younger generation that has grown up on Google.

Analysts of the Soviet Union did not make much use of formal tools or methods, except in some technical areas.[4] They tended to operate on the basis of their experience or that of their immediate work unit. Previous assessments or patterns were the point of departure, with analysts tending to look for information that would confirm those patterns —a tendency abetted by time pressure, which drove analysts toward early closure on open issues.

In the future, by contrast, analysis will need to make much wider use of method and technology, from aggregating expert views to searching, data mining, and pattern recognition. Data will be searched for the out of the ordinary, not just for confirming evidence. The key analytic choices will remain with analysts, but technology will provide memory even of hypotheses or data previously rejected by analysts, thus helping to notice what analysts are watching and what questions they are asking.

[3] For more detail, see Loch K. Johnson, *Bombs, Bugs, Drugs and Thugs: Intelligence and America's Quest for Security*, New York: New York University Press, 2000, especially Chapter 6.

[4] For a fascinating assessment by an anthropologist of intelligence's analytic processes, see Rob Johnston, *The Culture of Analytic Tradecraft: An Ethnography of the Intelligence Community*, Washington, D.C.: Central Intelligence Agency, Center for the Study of Intelligence, 2005. Dennis M. Gormley speaks in very similar ways about intelligence's lack of rigor, and he makes a number of thoughtful suggestions in "The Limits of Intelligence: Iraq's Lessons," *Survival*, Vol. 46, No. 3, Autumn 2004, p. 15ff.

Intelligence was not only stovepiped, it was organized hierarchically. Fritz Ermarth, a former chair of the NIC, once mused that intelligence analysis is still organized like the Roman legions. Intelligence, analysis in particular, needs to be in flat and highly networked organizations, and in that sense, creating "centers," more virtual than bricks-and-mortar, is the right direction. In solving puzzles about the Soviet Union, analysts worked alone or in small groups; in trying to understand terrorism, analysts need to be part of larger virtual networks, across specialties and agencies. Answering questions from a wide variety of customers may be best done with generalist analysts, but longer-term understanding requires deep specialists.

The needs of the future are not lost on U.S. intelligence agencies. Yet the press of the present is so intense, and the legacy of the past so powerful, that innovations so far have been piecemeal, if promising. Moving toward center-based organization will permit wider virtual networks to be put in place. But those centers will need to be accompanied by a wide range of experiments and innovations in analysis. And the groups inside intelligence that are thinking beyond the immediate—the NIC, for instance, or the CIA's Strategic Assessments Group—need to be reinforced.

Several examples suggest the range of experiments. The CIA's Sherman Kent Center has been working with the RAND Corporation to apply techniques of alternative analysis to terrorism and other transnational issues.[5] Alternative analysis seeks to challenge assumptions and widen the range of possible outcomes considered. Its purpose is to hedge against "groupthink" or premature consensus, and the natural tendency for analysts, like others, to search too narrowly, looking more intently for information that would confirm their prior hypotheses than data that would discredit them. The initiative has engaged experts not only in transnational issues (from both inside and outside the Intelligence Community) but also from a range of fields relevant to analytic thinking, such as cognitive psychology, psychiatry, organizational decisionmaking, product innovation, investment analysis, diplomatic history, and the like.

Instead of the traditional analytic process, understanding terrorism involves what Karl Weick calls "sense-making"—a more holistic, intuitive, and real-time process. It involves gaining a deep and broad understanding of a problem at hand in order to be able to discover emerging patterns. The objective is to connect the dots on a continuing basis in the knowledge that the nature and position of the dots are in constant flux. It may imply that, instead of deep expertise in a particular slice of a problem, what is required are many pairs of eyes looking at data for emerging threats. Sense-making by articulating hypotheses aloud before a group may advance the process. To be sure, the ideas are embryonic, and determining how to implement them is still a challenge.

A compelling example at the tactical end of analysis is called "multi-INT," the key to which is rapid iteration of information from more than one sensor. In one sense, multi-INT is not conceptually different from what intelligence calls "fusion" or even "all-source analysis," but in Afghanistan and Iraq it has involved analysts from NSA (handling SIGINT) and NGA (handling IMINT) in networks to permit very rapid responses in support of operational decisions made under great time pressure. In principle, though, multi-INT could be done within a single INT or even a single organization. In summer 2001, for instance, the Phoenix FBI agents interested in the flying school attended by Zacarias Moussaoui did not

[5] Fishbein and Treverton's *Making Sense of Transnational Threats* reports further on this work.

know that their colleagues had been interested in the same school two years earlier on suspicion that Osama bin Laden's pilot had trained there. In other words, the FBI did not know what it knew.

There is no shortage of tool-building going on—at the CIA's In-Q-Tel, and Advanced Technology Programs; at the Intelligence Community's Advanced Research and Development Activity, and Intelligence Information Innovation Center; or with the Pentagon's Defense Advanced Research Projects Agency. The initiatives are focused on mining large data sets but also remembering discarded hypotheses and seeing new patterns, as well as providing analysts with better ways of working together. As yet, however, the initiatives are scattered and are all too often driven by technology. With no clearinghouse for matching what analysts want and what technology can provide, innovations run the risk of remaining just fancy bits of technology, not real advances in analytic method.

So, a DNI ought to move to create a focal point for tool-building and innovation in using these tools.[6] If, for instance, all analysts had, more or less, similar workstations, that would facilitate moving them around the Intelligence Community, including into newly created centers. So, too, a focal point for learning lessons would make sense. Now, postmortems, like that over the error of U.S. estimates about WMD in Iraq, are usually conducted in the full glare of publicity and so run more toward assessing blame than learning how to do better.[7]

Dealing with New Professionals

All the intelligence agencies have grown dramatically since September 11, 2001, and this growth has provided wonderful opportunity. The young recruits are fearless and computer savvy. They will not stand for the information environments—compartmented, slow, and source driven—that current intelligence provides. Nor will they long be satisfied with work beats that amount to, as one new recruit put it, "a few square miles of Iraq."

To overstate for effect, this next generation will be fast, not slow; will perform parallel processing, not serial processing; will give pride of place to graphics, not text; will do random accessing, not step-by-step processing; will be connected, not stand-alone; will be active, not passive; will mix work and play; will be impatient for results; will mix fantasy and reality; and will very definitely see technology as a friend, not a foe. These ten characteristics can be a great future asset for intelligence or a considerable liability, depending on how these resources can be channeled to solve key intelligence challenges.

The Intelligence Community will not attract—or will soon lose—these young people if it does not accommodate to how they think and learn. Now, however, the community suffers because the tools and technologies are rarely, if ever, available in an open architecture system within the agencies, due to both legacy architecture and the constraints of security. Moreover, because young analysts do not have access to these commonly available tools, they

[6] This is akin to what my colleague, Leslie Lewis, calls a "warm base" of analysis—that is, one that is not collector centric but is built on a common framework, tools, and standards.

[7] The WMD Commission makes a parallel plea (see WMD Commission Report, p. 20). The CIA's Center for the Study of Intelligence, which published Johnston, *The Culture of Analytic Tradecraft*, would seem to be such a focal point, at least for the CIA, and it does do a number of histories. Yet its bias is that of historians and of covert operators, which tend to focus on the particularities of cases, not their possible lessons for the future.

not only will have less capability to do their jobs but also less and less familiarity with the tools that others outside government, or even their customers, are experimenting with and innovating.

At the same time, these new entrants are also untrained, and given the aging of the intelligence agencies, will lack for mentors. This problem could be turned to advantage if intelligence emulated the best Wall Street firms, which build "gray-green" teams, ones combining the savvy of veterans with the fearlessness of the new recruits. All the agencies will have to dramatically rethink how they deal with the lives and careers of their premier asset, their people. For instance, intelligence has been second only to military service as a lifetime career; lateral entry has been rare, particularly given the demands of security clearance, and a large percentage of those who have joined have stayed for an entire career. That will not be true into the future, though. Many young professionals will seek continual challenges. They will want to come and move on, perhaps returning later, pursuing what might be called "portfolio" careers, combining experiences in different sectors.[8] These people can open and enrich intelligence in just the ways it needs—but only if intelligence makes major changes in how it recruits, trains, and clears its people.

To take another example from the front end of the personnel cycle, as NSA and NGA have sought to reshape their missions from "gathering" to "hunting and gathering," they have encountered questions about both metrics for judging performance and the skills needed to perform.[9] Traditionally, the two agencies' initial processing and analysis were driven by what they collected; the process was gathering, what might be called "efficient production." An NSA veteran remembers having delivered each morning the take from "her frequencies"—several Soviet communications channels that NSA was monitoring—and her job was to process that take. Gathering will continue, in populating databases for example, and it will remain a kind of industrial process, albeit often a very sophisticated one. But the hunters, those who will reach out for data, looking across data sets and INTs—those engaged in what might be called "innovation operations"—probably will need first to be judged by different metrics than the producers and ultimately may be different people from those the agencies traditionally have sought. The "hunters" may need to be different from the "gatherers" in background, temperament, and training.

At present, training of analysts, in particular, is mostly on-the-job. More formal training is usually self-initiated; it does not result from any strategic planning of agency human resources. And almost all of it is stovepiped by agency, so analysts have little idea how their counterparts in other agencies actually do their work.

The 2004 bill does say the right things about training, emphasizing training across disciplines and training that would facilitate rotations of intelligence officers across agencies, and the WMD Commission recommends a National Intelligence University to promote jointness in training; that university has been created, at least on paper. However, the bill speaks of language training first, and then devotes most of its discussion of training to creating an Intelligence Community Scholarship Program, to provide stipends to university students in exchange for commitment to later service in intelligence.

[8] See Gregory F. Treverton and Tora K. Bikson, "New Challenges for International Leadership: Positioning the United States for the 21st Century," Santa Monica, Calif.: RAND Corporation, IP-233-IP, 2002.

[9] This discussion draws on work, as yet unpublished, by my colleagues Bruce Don and David Frelinger.

In interviews across the analytic agencies, none of the agencies had much familiarity with the analytic techniques of the others. In all, there tended to be a great deal of emphasis on "skill-level" certification, organizational processes, and writing and communication skills, and much less emphasis on analytic methods. There is a striking absence of common course components of emphasis on community-wide perspectives.[10]

Training is driven more by individual officials than by any strategic view of the agency or the Intelligence Community and its needs. That driver is one among several that leads toward an emphasis on *credentials* in training, perhaps at the expense of techniques more directly related to immediate analytic work. The CIA University, for instance, confers bachelor's and master's degrees, and the Joint Military Intelligence College offers both degrees as well. Surely, there is nothing wrong with granting degrees or other credentials; however, operators express concern that the schools are too distant from the needs of operators to be as helpful as they could be. From the side of the trainers, the concern was keeping up with the pace of needs—usually for specific new area or country knowledge—in circumstances in which the most knowledgeable "teachers" were precisely the experts in the highest immediate demand. The CIA's Sherman Kent School for Intelligence Analysis (part of CIA University), for instance, offers 80 courses on specialty disciplines.

Initiatives in tradecraft are also isolated. The Kent School, for instance, tries to keep up with best practices in the private sectors by sustaining four small teams that handle outreach; product evaluation; methods, including tools; and integration, that is, trying to keep the school's offerings matched to the needs of the CIA's Directorate of Intelligence. With the rush of immediate need, there are few opportunities or mechanisms for looking at tradecraft jointly, for understanding how other agencies do "analysis" and what might be learned from them or for developing centers of training excellence that develop comparative advantage instead of duplicating what has already been done elsewhere.

Regular joint training experiments and field tests in tradecraft—in both analysis and operations—would make sense, first, to create some shared methods across different tasks of intelligence. Now, although there is debate about how deeply the U.S. military should engage in espionage, would-be military spymasters train at CIA schools. Second, that training could begin to foster more of a sense of joint tradecraft, more community awareness on the part of the intelligence officers of what their counterparts in other agencies do or could do. And the process could contribute to advancing joint efforts more generally across the Intelligence Community.

The vision for intelligence training ought to emulate the military in being joint and integral to careers. In interviews, officials engaged in analysis endorsed the idea of some initial joint training of analysts but also said another joint training experience at, say, five years into their careers would be at least as valuable, since by then officials in one agency are more likely to need to work with other agencies. At present, intelligence is very far from that vision. For the most part, training is discretionary and individual, not required and strategic. Training is far from the expectation on the way up; indeed, too often the best intelligence officers are deterred from training by the imperative not to "leave the flagpole." And intelligence agencies do not have the slack in their officer ranks to permit officers to routinely depart for several months or even a year.

[10] The observations are echoed by Johnston, *The Culture of Analytic Tradecraft.*

How intelligence rewards its people will also have to change. Recent legislation has freed both DHS and DoD from many of the existing civil service constraints, and now more than half of the civilian employees of the federal government do not work under traditional civil service rules. Their managers now have much more latitude in rewarding performance. Similar provisions will apply to intelligence. So far, the experience has been that discretion to reward performance often goes unused; superiors hold back from taking the responsibility that would go with using the discretion they have, all the more so if performance metrics are ill-defined. And the last thing intelligence would want to do would be to fall back to the easier metrics, such as numbers of agent recruitments for CIA operators or PDB items for analysts.

Getting access to the best people will also mean rethinking what is done in-house and what can be reached outside government. Air Force intelligence, for instance, faces this challenge now in trading depth for breadth. Given the demands of the current business, there simply is no time to "train up" an analyst on a new current "hot button" issue with any serious depth. Existing programs for reaching outside only scratch the surface of what will be needed. For instance, the NIC is addressing the outsourced expert issue through its Global Expertise Resources Program (not very felicitously known by the acronym GERP), which preestablishes ties to subject-matter experts in critical areas throughout the world and facilitates their use to address key intelligence challenges. While now numbering roughly 40 academic experts with a goal of moving toward 100, other agencies worry that GERP will be too small, or its reservists too far from the needs of policy, to be very helpful.

A similar program—the Science and Technology Experts Program, or STEP—has been under way for a number of years, although with the same concerns about size and scope of the program relative to demand. As currently configured, STEP provides the NIC and others with access to a few dozen organizations with subject-matter experts in key areas of science and technology. This resource may be tapped for specific advise on intelligence problems. However, the resource is primarily amenable to limited-scope efforts of short duration. Program activities are manifestly consultative or advisory in nature and are difficult to translate into improved core capabilities for the Intelligence Community.

Intelligence needs open new ways for lateral entry, and in this regard the experience of the NIC is suggestive. In many areas, such as with top-flight economists, the government is and will continue to be hard-pressed to compete with the private sector. It will have difficulty attracting and retaining such talent for a lifelong career. But the NIC has recruited that talent for several-year stints. Top-flight professionals, many of whom have no more "worlds to conquer" where they are, can be drawn by some combination of patriotism and a desire to see how the government works.

Targeting Collection

"The intelligence failure in Iraq did not begin with faulty analysis. It began with a sweeping collection failure." So said the WMD Commission.[11] Every blue-ribbon panel calls for improving America's espionage, or HUMINT. The call is worthy, but expectations have to be reasonable. Beyond HUMINT, much of the U.S. collection architecture, such as satellites

[11] The quotations in this paragraph are from pp. 21 and 3, respectively, of the WMD Commission Report.

for imagery and eavesdropping, is pretty well understood by would-be adversaries. Those adversaries routinely camouflage sensitive activities when they know satellites are overhead. As a result, U.S. intelligence has too much data and too little information. New technical collection systems, especially for IMINT, threaten to overwhelm processing; yet, according to the WMD Commission, in the case of Iraq, both IMINT and SIGINT "produced precious little intelligence for the analysts to analyze." Thus, the long-term challenge for U.S. intelligence is to move away from passive surveillance techniques toward more directed collection and to shorten the cycle of innovation so as to be less predictable for would-be targets.

On the HUMINT side, however one judges the past half-century of U.S. espionage, doing better against tomorrow's much harder-to-track targets, such as terrorists, will not be easy. The required actions—such as making much more use of America's ethnic diversity or moving spying out of official cover—take time and money. For instance, the experience with spymasters under nonofficial cover, called "NOCs," so far has been mixed at best. Other countries have done better—the Soviet Union during the Cold War or China now—so patience is required. NOCs are expensive in both money and time to deploy and sustain, and because they have to actually live their cover, their time for recruiting spies is limited. Thus, they are costly for the information they provide. And, lacking the diplomatic immunity of official cover, recruiting spies as NOCs can be dangerous.

The difficulty of the task is not an argument against trying to do better.[12] It is, however, an argument against expecting too much. Successful espionage requires both patience and a willingness to traffic with unsavory characters. Neither comes easily to the American system. But the dilemma runs deeper: In many respects, effective spying requires attributes that are precisely the opposite of accountability in America's governance. Spying requires giving case officers in the field discretion. Government, by contrast, narrows discretion downward while pushing accountability upward.[13]

That means that, although we can do better at espionage, in the end we will still be dependent on friends—and even non-friends—who have access where we do not and perhaps may employ methods we would not. That will mean not just tending the rather clubby liaison relationships of the Cold War, most of them with fellow English-speaking nations, but engaging in specific and limited sharing and trading with such nations as Syria or Somalia, where the overlap of common interest is present but very limited.

Beyond espionage, intelligence faces the paradox of too much data but too little information. During the Cold War, information on the Soviet Union was in too short supply. Now, though, two things have changed. First, even though terrorists are secretive, information not secret—phone numbers, driver's licenses, and the like—is also relevant. That fact imposes on intelligence the need to develop ways to search huge amounts of data, a need all the harder for a community that, for reasons of secrecy and culture, has not been at the forefront of the information technology revolution.

Second, intelligence's own technical capabilities to produce secret information, such as with imagery from spy satellites, have mushroomed. Each new round of collection systems

[12] For an intriguing set of recommendations by a former CIA spymaster, see Robert Baer, "Wanted: Spies Unlike Us," *Foreign Policy*, Vol. 147, March/April 2005, pp. 66–77.

[13] I elaborated this point in Allen E. Goodman and Bruce Berkowitz, *The Need to Know*, Report of the Twentieth Century Fund Task Force on Covert Action and American Democracy, New York: Twentieth Century Fund, 1992, pp. 23–24.

dramatically increases the take, especially in imagery, but the capacity to process and analyze that take falls further and further behind.[14] As a result, the big collectors of IMINT and SIGINT—NGA and NSA—will be tempted to solve their processing problem by turning the fire hose of data on intelligence's analysts. After all, that is one way to make sure that they are not the culprits for the next intelligence failure; they passed the data, even if it was lost in torrents. A better balance is needed between investments in the emerging new-generation collection systems and enhanced forms of analytical capability. The latter means a greatly expanded investment in quality personnel and new technologies that assist analysts instead of overwhelming them. Put simply, terabits of data collected but unprocessed and unanalyzed are useless to the policymaker.

At the same time, all that collection risks producing less information even as it produces more data. Part of this is, as with analysis, due to the change in the nature of the target.[15] Spy satellites are good at seeing large armored formations but cannot "see" terrorist networks; easily follow small, fast-moving groups; or help us know what is going on inside chemical plants. Moreover, U.S. adversaries know a lot about U.S. techniques, often including the orbits of satellites, and so conceal activities. Some state adversaries, such as North Korea, have invested enormously in underground facilities to protect, but also to hide, their WMD or related activities.

SIGINT faces even sharper challenges, from digitizing, packet switching, fiber optics, and encryption.[16] Digitizing makes it possible to send huge amounts of information over a single channel and therefore vastly compounds the challenge of sorting out particular communications of interest. "Packet switching" means that the routing of a message may be changed in the middle of a communication and that the addressee of a message can be sent separately from the message itself, so matching addressee to message is difficult. With the improvement in cable transmission made possible through fiber optics, substantially fewer messages are sent into the open air, where satellites or ground stations can intercept them. The United States will have to get physically close to the communications channels it seeks to intercept.

On the technical side, U.S. collection will have to be much more targeted and more innovative. The Iraq case suggests that imagery and signals were driven by what capabilities existed, not by what was needed.[17] It also may be that the demands of "force protection"—in this case, detecting signs of threats to U.S. and allied pilots flying patrols in the northern and southern "no-fly" zones—limited the resources that could be devoted to understanding the WMD problem. The Community Management Staff has begun to sharpen targeting through its Collection Concepts Development Center. The center draws in knowledgeable outsiders to take a fresh look at collection with respect to a particular target or mission. Those reviews necessarily are driven by questions, not sources, and so begin to lash collection and analysis together around issues.

[14] On the mismatch between take and processing capacity, see Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2nd edition, Washington, D.C.: CQ Press, 2003, pp. 45–47.

[15] For a good discussion, see Chapter 7 of the WMD Commission Report.

[16] Treverton, *Reshaping National Intelligence*, p. 88.

[17] In his speech to the United Nations in early 2003, however, Secretary Colin Powell did play the transcript of a recorded conversation between an Iraqi general and colonel in the Republican Guard. The transcript of the speech is available at http://www.whitehouse.gov/news/releases/2003/02/20030205-1.html (as of September 2005).

Intelligence's impressive technical achievements during the Cold War are now pretty long in the tooth, and the primacy of satellites remains. The United States needs to broaden its collection means and shorten the cycle of innovation. As in Silicon Valley, innovations may remain secret, but not for long, and so intelligence will have to adapt faster than its targets if it is to stay ahead. For SIGINT, adapting means finding new ways to get very close to targets; for IMINT, it means using more, smaller satellites, or drones or stealth technology. It also means using new parts of the spectrum, such as hyperspectral imagery, to identify effluents from buildings or factories, as well as a range of technologies in what is called MASINT, or measurement and signature intelligence.

Pushing innovation and making better choices across the collection stovepipes is the chief rationale for having a DNI in the first place. It is the collectors that consume three-quarters of the $40 billion intelligence budget. If the DNI does not have the power to collapse the stovepipes, he can develop much more analytic capacity to make trade-offs across them, asking, for example: How do groundstations compare with satellites for particular SIGINT missions? Can HUMINT do a mission more cheaply? Many intelligence successes are the result of cooperation across the INTs: HUMINT or open sources may provide tips, which then lead to specific locations to be imaged and communications lines to be monitored. But to take advantage of such cooperation, analysts and collection managers need to know what the various INTs are doing and can do. The WMD Commission suggests that the DNI create an "integrated collection enterprise" for the Intelligence Community to provide for coordination across the entire cycle from planning new systems, to developing strategies for deploying existing systems against priority targets, to processing and exploiting information that is produced.

Rethink "Need to Know" and Other Security Procedures

Finally, while "information sharing" has become a mantra in the war on terror, existing procedures, with each intelligence agency controlling the information it produces, make it hard enough to share across U.S. intelligence, let alone get information to state and local authorities. More generally, innovations in intelligence *analysis* run smack into existing security procedures, which are designed to limit information to those with a "need to know," not share it. Yet new analytic insights are likely to arise precisely from those who come to the information with a fresh perspective, who have *no* need to know. The fundamental challenge is reshaping how the U.S. government thinks of information, and how information should be used and controlled. Both commissions deserve credit for at least raising the issue. In addressing it, the language of "information sharing" is both tepid and misleading.[18]

Current rhetoric about the "transformation" of the Intelligence Community celebrates exploiting information derived from the full spectrum of secret and open courses. Such terms as "multi-intelligence," or "multi-INT," and "fusion analysis" are the associated catch phrases, and another favorite is "connecting the dots." Yet, again, every innovation requires more sharing. As a result, paradoxically, some of the most interesting multi-INT experiments have not been virtual but rather have depended on place. That is, so long as they

[18] The WMD Commission recommends jettisoning that language, not least because it implies that agencies, not the government, own information (WMD Commission Report, p. 29).

were small and experimental, they could get license to operate "within the security fence," sharing information in ways that the originating agencies probably would not have permitted on a larger scale. In one example, an analyst literally faces a handful of computer screens, and "fuses" information by rolling his chair from one to the next—what might be called "wheeled fusion."

In public presentation, the challenge of sharing intelligence with state and local authorities, down to the cop on the beat, often is portrayed as a problem of technology. It is not. Technology can help. But the challenge is one of policy, not hardware. There is a clear need for more candor between the administration and Congress over the costs of the current information security system.

From the outside, the security issues appear daunting, but insiders seldom mention them. They are so used to these issues that they hardly notice—a sad indicator of how hard change will be. In one sense, the problem of security is less pressing now, at least in principle. During the Cold War, intelligence was very dependent on a small number of collectors, so any single-point exposure was deeply damaging. Arguably, that is less so now with many, varied targets and much more information. Even if that is true, however, it still means that intelligence will have to recognize, as Silicon Valley has, that innovations that confer advantage are fleeting. If advantage is to be maintained, it will require a short cycle in producing new innovations.

The 9/11 Commission recognizes that the issues are less technical than policy related in nature. It recommends creating a government-wide "trusted information network" to share information horizontally, on the model suggested by a recent task force organized by the Markle Foundation.[19] For the WMD Commission, the December bill's provisions on that score, though, raise as many questions as they answer. The bill would create a program manager to build such a network for the war on terrorism; yet that manager would sit outside the Intelligence Community and report to the President. Meanwhile, the DNI would remain responsible for facilitating the sharing of all information within the Intelligence Community.

Reshaping security to effectively confront the threats ahead requires perhaps the ultimate change in culture. It will not come soon. In the meantime, a number of smaller proposals can at least ameliorate immediate problems. For instance, intelligence analysts, like other professionals, want to play at the top of their games, so their reports inevitably begin with the most classified—and thus least sharable—information. The 9/11 Commission suggests the opposite, starting any report by separating information from sources and writing first at the level that can be most easily shared. If intelligence consumers wanted more, they could query the system under whatever rules were in place, leaving an audit trail of requests. Now many, perhaps most, potential consumers would not even know what to ask for.

Already, many agencies have reached out for translators into pools of people they would not have tapped before, immigrants who have spent much of their adult lives abroad. Certainly, it is possible to imagine different kinds of clearances for different kinds of jobs. So, too, the military is creative during coalition operations in using "tear line" intelligence, so that information can be separated from indications about the source and transferred to non-

[19] See *Creating a Trusted Network for Homeland Security*, Second Report of the Markle Foundation Task Force, December 2003. Online at http://www.markletaskforce.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php (as of September 2005).

American coalition partners. The FBI and DHS should be comparably creative in thinking of ways to get information to uncleared partners. Now, the principal means the federal government has for working with state and local authorities are the FBI joint terrorism task forces. Yet those are built around FBI communications and, therefore, require state and local participants to be cleared at the top-secret level.

On the collection side, the terrorist threat to the homeland is impelling intelligence—in particular, the FBI and DHS—to think of their officers as "embedded collectors." Before September 11, 2001, FBI agents, for instance, collected a lot of information but concentrated on the portion that was immediately relevant to the specific case they were investigating. As embedded collectors, they would recognize that information they collect has value beyond the case, to others if not immediately to them. In addition to the FBI, DHS has 18,000 agents in Customs and Border Protection, 15,000 employees in Citizenship and Immigration Services, and 48,000 screeners in the Transportation Security Administration—all potential intelligence collectors—not to mention 600,000 state and local law enforcement officers.

As yet, DHS has no mandate to collect intelligence, and the word "collection" remains a taboo, but the capacity exists. To be sure, embedded collectors raise a host of civil liberties issues. And, more practically, those collectors need to know what to look for and how to pass on what they see. Gilman Louie, president of In-Q-Tel, the CIA's high-tech venture capital company, likens the need to having a "soda straw" reaching down to the cop on the beat. Now, however, there is no infrastructure for the straw, let alone guidance and policy to govern what should be pushed or pulled through that straw.

Coda: Congressional Oversight

The December bill is a poignant reminder that Congress finds it easier to organize the Executive Branch than itself. DHS officials now appear before a total of 88 committees and subcommittees of Congress. It took a bitter battle in the House to create a permanent Homeland Security Committee in 2005, and even that battle had the effect of creating one more point of oversight; for the most part, it did not strip existing committees of their role. For intelligence, the situation is not quite so extreme, but the 9/11 Commission suggested that if a single DNI is to oversee the entire community—and to preside over funding for all of it—Congress also should concentrate its oversight. Accordingly, the commission would call on Congress to renew its commitments from the 1970s, having either a single joint committee to oversee intelligence (on the model of the old Atomic Energy Committee) or single committees in each house. Like the House Homeland Security Committee after them, the intelligence committees were never given the monopoly that was intended at their creation, and through the years even more committees have become involved.

The 9/11 Commission also would revamp ideas from the 1970s agreements in several other ways. To represent other committees with interests in the field, the new oversight committee or committees would revert to the practice of having a member who also serves on each of the following committees or subcommittees: Armed Services, Judiciary, Foreign Affairs, and Defense Appropriations. To promote continuity and expertise, oversight committee members should serve indefinitely on the new intelligence committees. The new committees should be smaller—perhaps seven or nine members in each house—so that each member feels a greater sense of responsibility and accountability for the quality of the committee's work.

Here, too, the arguments are long-standing, running back to the congressional investigations of the 1970s. Those investigations, one in each house, were touched off by concerns that intelligence agencies had violated the rights of Americans, particularly through their involvement in events surrounding the Watergate break-in and by revelations of covert CIA interventions in Chile's politics. These events were a first-ever lifting of the veil on U.S. intelligence.[20]

However, changing times reshuffle the arguments. Surely, the idea of having real focal points is the right one. The objective was identical in the 1970s, but it was never fully achieved and has eroded since then as more committees have gotten into the act. In those days, the model favored by the 9/11 Commission, a single committee for both houses on the Atomic Energy Committee model, was not in favor, since it was regarded as having become the captive of the agency it oversaw. The fear that permanent committee members might become too cozy with the agencies they oversaw also led Congress in the 1970s to give the intelligence committees rotating memberships.

Now, however, those memories are distant, and the need for focal points is more intense. To try to achieve those focal points, the 9/11 Commission also favors the 1970s' practice of appointing members from other committees with stakes in intelligence to the oversight committees. So, too, the experiences of 2001 and of the faulty estimates in the run-up to the Iraq war seem to highlight the need for experience on the oversight committees, outweighing concerns over cooption, and so the commission favors open-ended assignments to the committee or committees, not rotating ones. But these are details. The real challenge for Congress is not to lag the Executive Branch too much in its own reshaping in preparing for the intelligence challenges of the 21st century.

[20] In the spirit of full disclosure, I was a staff member of the Senate committee, often called the Church Committee after its chair, Senator Frank Church (D-Ida.). For an assessment by a fellow staffer, see Loch K. Johnson, "Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee," *Public Administration Review*, Vol. 64, January 2004, pp. 3–14.