CHAPTER SEVEN
COLLECTION

Summary & Recommendations

The collection of information is the foundation for everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect information—as our Iraq study demonstrated—turns analysis into guesswork. And as our review demonstrates, the Intelligence Community's human and technical intelligence collection agencies have collected far too little information on many of the issues we care about most.

This chapter sets forth our recommendations for improving the collection capabilities of our Intelligence Community so that it is better equipped to confront today's diffuse, elusive, and ever-changing intelligence challenges. These recommendations fall into two categories: those focused on improving the performance of particular collection agencies, and those aimed at integrating the management of collection across the Intelligence Community. Among other suggestions, we recommend that the DNI:

- Create an "integrated collection enterprise"—that is, a management structure that ensures that the Intelligence Community's decentralized collection capabilities are developed in a manner that is consistent with long-term strategic intelligence priorities, and are deployed in a coordinated way against today's intelligence targets;
- Encourage the development of new and innovative human intelligence collection techniques, and empower the CIA to coordinate the full spectrum of human intelligence activities performed in the Intelligence Community; and
- Establish an Open Source Directorate in the CIA responsible for collecting and storing open source information, and developing or incorporating commercial tools to assist users in data searches—including those in foreign languages.

INTRODUCTION

The Intelligence Community exists, first and foremost, to collect information vital to the national security of the United States. This may seem self-evident, but it bears restating—for as our case studies demonstrate, there are simply too many gaps in our understanding of too many serious national security threats. Our Iraq case study found a near complete failure across all of the Intelligence Community's collection disciplines—from those who collect human intelligence, to the technical collection agencies that take satellite photographs and intercept communications—to gather valuable information on Saddam Hussein's weapons capabilities. And our broader review found that Iraq was not an isolated case. From Iran's pursuit of nuclear weapons to the inner workings of al-Qa'ida, the Intelligence Community frequently admitted to us that it lacks answers.

The collection challenges facing the Intelligence Community are certainly daunting. In addition to maintaining the ability to penetrate closed societies—a capability that proved essential to the conduct of foreign policy during the Cold War and that remains vital today with regard to states including China, North Korea, and Iran—the Community also faces the imperative of collecting against secretive transnational organizations that operate globally. At the same time, modern warfare requires that national intelligence collectors both support strategic planning needs and offer real-time assistance to military operations. In short, the Community is facing unprecedented demands to do it all, and to do it all very well.

It is clear that the old ways of doing business will not suffice to meet these challenges. For example, the "traditional" model for collecting human intelligence is ill-suited to confront some of today's most critical intelligence challenges. And traditional technical collection techniques have been degraded by the pace of change in telecommunications technology and by our adversaries' increasing awareness of our capabilities. It therefore came as no surprise to us when we found that many recent intelligence successes resulted from more innovative collection techniques. But as these innovation efforts are still episodic and far too rare, in this chapter we offer recommendations aimed at encouraging our intelligence agencies to develop new ways of collecting information—ranging from methods for conducting human intelligence, to finding technologies for exploiting the massive amount of "open source"

information now available on the Internet and in other publicly available sources.

But to focus only on developing new techniques would be to confront only half of the collection challenge. Of equal importance—and consistent with our call for greater integration throughout the Intelligence Community—we found that collectors too often operate independently. Our largely autonomous collection agencies have not been accountable to any central authority within the Intelligence Community for the investments they make or the quality of intelligence they collect. Moreover, because they do not coordinate their activities, opportunities for highly promising collaborative collection are often missed. Therefore, we also propose that the Intelligence Community's collection capabilities be managed as an "integrated collection enterprise"—that is, we need a collection process that is strategically managed and coordinated at every step, from investment in research and development, to the acquisition of technical systems, to the formulation and implementation of coordinated cross-agency strategies for deploying our collection resources.

Despite the difficulty and diversity of the challenges facing the Intelligence Community, the excuse "it's too hard" plainly will not suffice. We must reconfigure the Community's collection capabilities in ways that enable it to reduce uncertainty against key intelligence threats. This chapter offers our recommendations for accomplishing this objective.

THE TARGETING CHALLENGE

Our recommendations are designed to increase the Intelligence Community's ability to collect against today's targets as well as expected targets of the future. As a starting point, however, it is worth considering how our collection system got where it is today, and why the rapidly changing nature of many threats makes that system so inadequate.

The Cold War

Throughout the Cold War, the United States focused its collection efforts against monolithic Communist powers—the Soviet Union and China—and their proxy states. These targets had sizeable military and industrial complexes that our satellites could observe, and they had hierarchical institutions, predictable communications procedures, and reporting behavior that we could

selectively target for eavesdropping. As a result, although penetration took time and was far from perfect, on the whole the Intelligence Community gained an impressive understanding of our main adversaries.

During this period, a number of intelligence agencies—the National Security Agency, the National Reconnaissance Office, and others—developed around the various technologies and disciplines used to collect against these targets.[1] These agencies were largely independent entities capable of determining their own strategies with only general guidance from above. As a general matter, they engaged in limited collaborative collection, and each (unsurprisingly) tended to invest in the research and development of technologies for collecting on the traditional Cold War targets. They did not (nor, perhaps, could they) anticipate the very different threats that we face today.

Today's Targets

In contrast to the Cold War, today's collection environment is characterized by a wider spectrum of threats and targets. For example, non-state actors such as al-Qa'ida present a new type of asymmetric menace. They operate globally, blending into local society and using informal networks for support. Locating and tracking dispersed terrorists and guerrilla fighters hiding in an urban environment—rather than massed armored forces on a European battlefield—typifies the type of collection problems the Intelligence Community faces today.[2] Such dispersed targets can, and often do, communicate chiefly through methods that are difficult to detect and that some of our collection systems are poorly suited to penetrate. In sum, today's threats are quick, quiet, and hidden.

Of course, state actors like Russia, China, and North Korea also continue to require attention. But for several reasons, penetrating these targets has also become more difficult than ever before. For example, authorized and unauthorized disclosures of U.S. sources and methods have significantly impaired the effectiveness of our collection systems. Put simply, our adversaries have learned much about what we can see and hear, and have predictably taken steps to thwart our efforts.[3] In addition, the changing face of weapons technology now means that certain weapons types, particularly biological and chemical weapons, can be produced in a manner that is difficult or impossible to detect.[4] All of this implies that the Community's effectiveness will continue to decline in the coming years unless concerted change occurs.[5]

Addressing Today's Collection Demands

It's not just that targets have changed; demands for collection have also shifted. Most significantly, since the first Gulf War, U.S. military requirements for national intelligence have spiked.

In the not-too-distant future, the U.S. military hopes to achieve a common operating picture of the battlefield in real time using a diverse set of tactical, national, and commercial sensors and communication technologies. This force transformation will create new requirements for collection and necessitate new approaches to fusing and integrating data to enable real-time analysis. And although the military's vision is not yet a reality, current demands have already put a strain on finite collection capabilities.

As a result, military requirements on national collection systems (such as satellites) have already diminished our effectiveness with respect to other targets important to national decisionmakers. For example, a study of why the Intelligence Community failed to warn of the surprise nuclear tests in India in May 1998 found that limited collection on India test sites was explained, in part, by its low priority owing to competing military requirements.[6] More recently, we found that support to current military operations in Iraq diverted imagery collection resources that would otherwise have been available to obtain information on nuclear developments on other priority targets in the region.

Regrettably, the Intelligence Community does not currently have a systematic process for balancing these competing interests. Today, the Assistant DCI for Collection and the Under Secretary of Defense for Intelligence meet frequently to discuss collection issues, including the allocation of national intelligence systems to support the needs of the military. However, neither individual has the requisite authority or resources to routinely develop and direct the implementation of integrated target development strategies.[7] As a result, the Intelligence Community has tended not to use its available collection systems efficiently.

This inefficiency is merely illustrative of a larger problem—the absence of methods for prioritizing and coordinating our Intelligence Community's decentralized collection capabilities. No office or individual sets long-term research and development priorities, acquires necessary capabilities, and formulates and implements an integrated collection strategy from a Community-

wide perspective. Instead, each of these functions is run by a panoply of different intelligence collection organizations.

Our case study of Iraq found that such disaggregation sometimes undermined effective intelligence gathering. Other studies we conducted, including those involving Iran's nuclear program and North Korea, further concluded that the current collection system has limited ability to engage in long-term, coordinated planning on existing threats, let alone to anticipate surprises. As a result, intelligence collection appears to be consistently behind the curve in identifying change, and it is usually positioned to be reactive rather than proactive—when it needs to be both.

Many of these observations—and our associated recommendations—are not new. Several decades of studies of the Intelligence Community have identified the lack of a unified, coherent collection process as a major shortcoming of the Community.[8] These studies recognized that under the existing system, no one other than the President, who obviously lacks the time for such a detailed task, has the clear authority to direct all of the nation's collection assets. This absence of central authority has impeded the development and implementation of unified strategies that operate existing collection assets against "hard targets."[9] In today's threat environment, we cannot wait decades longer to remedy these problems.

CREATING AN "INTEGRATED COLLECTION ENTERPRISE"

Recommendation 1

The DNI should create a new management structure within the Office of the DNI that manages collection as an "integrated collection enterprise." Such an integrated approach should include coordinated target development, collection management, data management, strategic planning and investment, and the development of new collection techniques.

Intelligence collection is a massive endeavor. In order to collect effectively, the Intelligence Community must develop, buy, and operate collection systems, manage the data that the systems collect, and plan for the acquisition of future systems. It is this cradle-to-grave process that we refer to as the "col-

lection enterprise." As the following makes clear, the Mission Managers we proposed in our chapter on management will play an integral role in nearly every facet of this integrated structure. There are five key components to this enterprise:

Target development: The process of defining collection priorities, determining existing collection gaps, and developing integrated collection strategies to address those gaps;

Collection management: Ensuring the effective implementation of the integrated collection strategies across the collection disciplines;

Data management: Supervising the processing, exploitation, movement, and analysis of data that is collected through each of the different collection disciplines;

Strategic planning and investment: Evaluating different investment alternatives, considering budgetary tradeoffs, and establishing long-term acquisition strategies; and

Developing new collection techniques: Evaluating current collection methods, designing new methods (including new platforms for human intelligence), and establishing research and development programs to fill intelligence needs.

As we have already discussed, each of the five functions we identify is currently performed primarily within individual collection agencies. The goal of our recommendation is to create an integrated collection process that performs each of these functions from the perspective of the *entire* Intelligence Community, rather than individual agencies. This is not to say that there are no benefits to the current decentralized approach to intelligence collection. We recognize, for example, that each agency understands its own capabilities best and is, in many ways, able to optimize its own efforts.

Our recommendation therefore attempts to build on these strengths. The new integrated enterprise will draw on the technical expertise possessed by each collector, but will also demand that agencies work together to ensure that all forms of collection are used where they are most needed and effective. We also do not expect the new collection enterprise to displace existing

personal relationships between collectors and analysts that allow analysts to provide additional clarifications or tasking. We do expect, however, that the centralized process we propose would ensure that the resources of our collection agencies are marshaled in a more strategic, cost-effective, and coordinated way.

We consider each of the key components of this integrated enterprise in turn.

Integrated Target Development

Recommendation 2

Target Development Boards, which would be chaired by the Mission Managers, should develop collection requirements and strategies and evaluate collectors' responsiveness to these needs.

Current collection processes are unique to each collection discipline and are often supported by complex and opaque "requirements systems." This typically means that in order to ask a collection agency to gather intelligence on a particular issue, analysts must forward their intelligence needs to their organization's collection managers or to discipline-specific Community collection committees, which in turn send collection requirements to specific collection agencies. Some analysts may also submit informal, *ad hoc* requests to their working-level associates and counterparts in collection organizations. Each collection agency then works independently to satisfy the "customer"—meaning, in this case, the analyst.

This rather haphazard process is occasionally prodded or refined by the intervention of the Assistant Director of Central Intelligence for Collection and his National Intelligence Collection Board (NICB), whose members represent the collection agencies. The board members meet to discuss and review some high-priority intelligence issues and the efforts by individual collection agencies to fulfill the associated collection requirements. We believe that this process has shown itself to be inadequate to the collection challenges facing the Community today, and that a more integrated strategy—one that would consolidate information needs and collection capabilities in one forum—would be a dramatic leap forward. We recommend the establishment of standing Target Development Boards for this purpose.

In our chapter on management (Chapter 6), we recommend that the DNI establish several "Mission Managers" who would be responsible for managing both analysis and collection on a particular intelligence target. Each Mission Manager would chair a Target Development Board, which would precisely define and prioritize information needs for that Mission Manager's subject area, determine existing intelligence gaps, and develop collection strategies to address them. As this list of responsibilities suggests, the boards would comprise both analysts and collectors from all relevant agencies and the military. Board members would have full visibility into the range of collection capabilities (including, as needed, those that are especially sensitive). The boards, led by the Mission Manager, would develop collection strategies that would serve as the blueprint for the Community's collection efforts. The boards would also provide a forum for discussing the optimal way to conduct those efforts. Ultimately, Target Development Boards would assess whether collectors have fulfilled their information needs[10] —and if they determine that existing collection capabilities cannot fulfill these requirements, Mission Managers could recommend that research and development of particular new sources and technologies are needed.

We have purposely avoided addressing the question of comprehensively listing which issues should be served by Mission Managers. In our view, the new DNI will be best situated to evaluate what issues are most pressing and therefore require Mission Managers. That being said, we believe the DNI should develop clear processes for defining the scope of responsibility for new Mission Managers and for phasing out—or "sunsetting"—Mission Managers whose missions no longer warrant such attention. We think this last point is critical, for one of the advantages we see in Mission Managers, as opposed to more permanent centers, is the flexibility they offer the DNI to adjust to shifting priorities. Finally, the DNI might consider establishing a "Global Issues Mission Manager" to serve as a "catch-all" for any number of issues that require special attention yet do not require their own Mission Manager.

Strategic Management of Collection

Target Development Boards would send baseline requirements for their issue directly to collection agencies (*e.g.*, NSA, NGA, CIA). In addition, a consolidated, prioritized list of all the target board requirements—reflecting the priorities of the President, other key decisionmakers, and the military—would be

developed on a periodic basis to provide strategic guidance to collectors as to the nation's most important information needs and to ensure a balance is maintained between national intelligence collection support to military operations and other national priorities.

The part of the DNI's office responsible for managing national intelligence collection resources would work with the Mission Managers to ensure that their consolidated collection strategies are executed efficiently, and would resolve conflicting requirements. This part of the DNI's office would be best suited to strategically oversee the implementation of the integrated Target Development Board strategies by guaranteeing that collection agencies were in fact targeting the identified priorities and making sure that each collection system was targeting the intelligence gaps that it is best suited to address. This same entity could monitor overall developments within the collection organizations and would assist the Mission Managers by keeping them informed of collection activities and helping to evaluate the performance of collectors.

Introducing Mission Managers, Target Development Boards, and a strategic management element to the collection process would thus address several specific, serious flaws that were identified in our case studies by providing a permanent mechanism for identifying current and future intelligence gaps and pairing those gaps with the capabilities required to fill them, a forum for developing strategies that optimize resources by reducing redundancy and maximizing opportunities to use the various collection disciplines in tandem or complimentary fashion, and a formalized system for ironing out competing collection priorities across the Community.

Targeting in an Integrated Fashion

What might the target development and strategic management components of the integrated collection enterprise mean in practice? We anticipate that the basic process might work much as described in the following scenario if the DNI were to designate a Mission Manager for Country X:

Targeting in an Integrated Fashion (Continued)

We envision that the Country X Mission Manager, in conjunction with analysts and the Country X Target Development Board, will identify the most important subject matter areas relating to Country X's nuclear program. The Target Development Board will then study all available collection capabilities against the target and craft a strategy that matches those capabilities from across the Community to the intelligence "gaps" we have in our understanding of Country X's program. If collectors come up short in filling these "gaps," the Mission Manager may recommend more aggressive collection techniques involving higher risk strategies. Because it is a standing entity, the Target Development Board will be able to quickly revisit priorities in response to changing events, and adjust the collection strategy correspondingly.

Having developed a collection strategy, the Mission Manager then will forward collection requirements to various collection agencies—NSA, NRO, CIA, DIA, and others. A collection-focused office in the DNI's office (perhaps a Deputy DNI for Collection), assisted by the Mission Manager, will work to ensure that the collection agencies implement the collection strategy, help them fine-tune it where necessary to encourage complementary collection strategies, and seek to avoid redundant efforts.

As our case studies suggest, there will likely be conflicts over resources. For instance, the Mission Manager for Terrorism may argue that more satellite time should be directed toward targets of interest in Country Y, and the DNI's designee will be forced to make hard choices. The Mission Manager and the DNI's appropriate deputy will remain involved in the day-to-day monitoring of collection efforts to coordinate with the collection agencies and ensure that Country X issues are addressed—or that an inability to collect on the Country X target, due to a need to focus collection resources elsewhere, is factored into Community-wide assessments.

Integrated Data Management

The collection enterprise does not stop with the actual collection of information. It is also about moving that information into the collection agencies, processing and exploiting the data, disseminating it to analysts and, increasingly, directly to users. All of this requires a sophisticated information infrastructure that allows for the manipulation of huge volumes of data. (Chapter 9 (Information Sharing) deals with the necessity of removing barriers to information

flow *among* agencies.) But a precondition to improving Community-wide information sharing is the development of common data management infrastructures *within* individual agencies that can be integrated with the Community as a whole. Only then will different collection agencies be able to collaborate and effectively maximize the advantages of multi-discipline collection.[11]

The idea that an integrated data management infrastructure will allow collection agencies to work more closely with one another is far from new. In fact, we must commend the current Directors of NSA and NGA—Lieutenant General Michael Hayden and Lieutenant General (Ret.) James Clapper—for their visionary efforts to create interfacing data management tools and methodologies for their two agencies. Regrettably, the directors' efforts have been stymied by two problems. First, the agency bureaucracies have tended to focus on their local needs versus the more global, Community-wide needs. Second, both agencies have been unable to successfully complete the necessary large-scale acquisition contracts.[12]

The lack of progress in developing new information infrastructures, and the failure to develop common information technology standards across the Community, will continue to be a major impediment to an integrated collection enterprise. Without a Community-wide plan, we fear that individual agencies will continue to invest—and waste—large amounts of resources in underperforming information infrastructures that cannot be integrated easily with other information systems across the Community.

We therefore propose, consistent with the *Intelligence Reform and Terrorism Prevention Act's* directive,[13] that the DNI develop a strategic plan for enabling collaboration and information sharing among collection agencies. This plan would identify the requirements for a Community-wide information infrastructure, set common standards for promoting information sharing techniques such as data-tagging, and develop guidance on new tools and methods for exploiting and processing collected data.

Integrated Strategic Planning and Investment

Technical collection currently accounts for roughly half of the intelligence budget.[14] One of the obstacles to achieving an integrated collection system is the fragmented nature of the intelligence budget, which is divided along pro-

grammatic lines and largely committed to legacy systems. Previous attempts to develop Community-wide budget priorities have met resistance from individual intelligence organizations, which naturally prefer the autonomy they enjoy under the current system.

Without a single individual or office to overcome these barriers, the Intelligence Community's enormous investment in technical collection has been, in some cases, duplicative and slow to respond to changed conditions; it has also provided the United States with inadequate capabilities to penetrate targets. Integrating strategic planning and investment would give a single office authority to look across collection agencies and advise the DNI on where to invest the Community's resources.

We believe the DNI should establish an office with requisite authorities to develop a strategic investment plan for Community-wide collection capabilities. This body would:

- Review, evaluate, and oversee National Intelligence Program (NIP) collection programs and budgets as part of the DNI's annual review process, including strategic investment for development of future collection concepts and associated processing, exploitation, and analysis capabilities;

- Conduct evaluations of collection investment alternatives across disciplines;

- Allocate strategic investments to develop new sources and methods;

- Collaborate with designees of the Secretary of Defense to ensure the effective integration of collection systems in the NIP, Joint Military Intelligence Program (JMIP), and Tactical Intelligence and Related Activities (TIARA) budgets;

- Ensure that investments in collection, processing, exploitation, and dissemination technologies are appropriately balanced; and

- Ensure appropriate funding for strategic investment priorities and, to the extent possible, ensure that such funds are not obtained through supplemental funding.

Integrated Development of New Collection Techniques

The primary obstacle to developing and implementing a sound research and development program is the same as that which stands in the way of an integrated strategic investment plan. Today there is no single official empowered to manage the Community's overall research and development needs. A single person should have authority to assess alternative options, select among competing priorities, choose solutions, and direct appropriate research and development initiatives to solve collection problems.

To establish an integrated approach to research and development across the Intelligence Community, the DNI should create an office responsible for assessing collection technology needs and developing a unified research and development strategy. This structure should be responsible for the following functions:

- Assessing program and technology gaps and proposing solutions;
- Developing and defining collection research and development strategies and plans;
- Developing and implementing innovative approaches for technical, operational, and exploitation functions related to collection;
- Working with the Office of the DNI's Director of Science and Technology to ensure that the national technology community—including the government, national labs, academia, and the commercial sector—has effective processes to recognize future threats and opportunities, and to help develop new and effective collection approaches;
- Ensuring the development of collection sensors, platforms, systems, and architectures that show substantial promise of defeating foreign denial and deception programs; and
- Ensuring that agencies have sufficient research and development funds to take advantage of innovative new approaches in collection and analysis.

This office should also be equipped with a significant budget in order to fund independent research without first seeking consensus from the collection agencies' various research and development units. It should also be given

authority to oversee and recommend modifications to the research and development budgets of those units. We believe that the DNI should determine how these collection-specific research and development needs should relate to the newly-created Director of Science and Technology. [15]

Even with the creation of an office dedicated to Community-wide research and development, we remain concerned that the DNI may have difficulty ensuring unity of effort.[16] The DNI does not have control over significant portions of the research and development budget contained in JMIP and TIARA. Nor does the new legislation resolve existing conflicts between the authorities of the DNI and Secretary of Defense for funding and managing programs within the NIP, JMIP, and TIARA. We have learned of several instances in which important efforts were stalled by conflicts of authority. For example, at least one major technical collection initiative—one that we cannot describe in our unclassified report—has been in limbo for over two years because the Intelligence Community and Defense Department cannot agree on a single set of requirements, mission scenarios, funding, operational control, and integration with other technical collection programs. Our recommendation, therefore, is only a half-step toward the needed solution; as we have noted elsewhere (see Chapter 6, Management), close cooperation with the Defense Department is also required.

IMPROVING THE PERFORMANCE OF INDIVIDUAL COLLECTION DISCIPLINES

Human Intelligence Collection

Human intelligence serves policymakers by providing a unique window into our targets' most guarded intentions, plans, and programs. During the Cold War, intelligence from GRU Colonel Oleg Penkovskiy proved critical to our management and eventual resolution of the Cuban missile crisis. Later, Polish Colonel Ryszard Kuklinsky provided us with highly secret war plans from the Soviet Union. The recent penetration of the A.Q. Khan nuclear proliferation network is another example of an impressive human intelligence achievement.

As the President himself has observed, the United States desperately needs human sources to confront today's intelligence challenges.[17] To its credit, the Intelligence Community has, since September 11, undertaken efforts to rise to

the President's challenge and redirect human intelligence collection toward today's threats. But as our case studies make clear, in the context of hard targets like Iraq, Iran, North Korea, and al-Qa'ida, human intelligence is still not delivering the goods. We have identified numerous reasons for this:

Losing human intelligence resources. Since the dissolution of the Soviet Union, the loss of human intelligence resources has brought the Community well below optimal strength. In the 1990s, CIA's Directorate of Operations (DO) experienced an appreciable decline in its career service rolls, including a significant decline in operations officers.[18] Similarly, DIA's Defense HUMINT service lost hundreds of billets between 1995 and 2001.[19] The Community has suffered a hemorrhage of irreplaceable experience.

The threat has changed, but we have not adapted. Post-Cold War targets—which include numerous "denied areas" and elusive non-state terror organizations—require our human intelligence agencies to develop different skill sets. We believe that human intelligence collectors have been too slow to respond to this sea change in operational requirements.

The hardest conventional targets remain largely impenetrable. Traditional state targets remain resistant to human penetrations. Our foes tend to be police states and totalitarian dictatorships—regimes that typically excel at countering espionage against them. Closed states like North Korea and Saddam Hussein's Iraq have countered U.S. collection efforts with, among other tools, pervasive counterintelligence and security apparatuses. Our case studies—including both Iraq (Chapter 1) and our classified studies of other "closed societies"—starkly illustrate human intelligence collectors' continuing difficulty in penetrating these targets. Intelligence Community coordination issues, bureaucratic risk aversion, and highly inadequate cover diversification have all retarded progress against these key targets.

Human intelligence collection is uncoordinated and lacks common standards. Minimal coordination among elements in the past sufficed when the CIA, FBI, and the Defense Department had more distinct missions, but lines of authority have blurred due to these agencies' responses to the imperatives of the terrorist threat. Both the FBI and the Defense Department's Special Operations Forces are major new players, and DIA has expanded its existing human intelligence service. There is considerable value in the new resources

and perspectives that these new players bring, but there are risks as well. These risks can only be addressed through greater coordination.

Some human intelligence agencies do a poor job of validating human sources. The story of "Curveball"—the human source who lied to the Intelligence Community about Iraq's biological weapons programs—is an all-too-familiar one. Every agency that collects human intelligence has been burned in the past by false reporting; indeed, the Intelligence Community has been completely fooled several times by large-scale double-agent operations run by, among others, the Cubans, East Germans, and Soviets. It is therefore critical that our human intelligence agencies have excellent practices of validating and vetting their sources.

We believe that these deficiencies in validating sources demonstrate that the Intelligence Community needs to change fundamentally the way it conducts the human intelligence mission. Specifically, we recommend: (1) that the Community develop and increase the use of new human intelligence collection methods; (2) that a new Human Intelligence Directorate be created within the CIA and that it be given the lead in coordinating the full spectrum of human intelligence activities performed Community-wide; (3) that steps be taken to professionalize the Intelligence Community's cadre of human intelligence officers; and (4) that human intelligence training be diversified and expanded to broaden expertise and reduce seemingly intractable training bottlenecks.

Coordinating Human Intelligence

Recommendation 3

Strengthen the CIA's authority to manage and coordinate overseas human intelligence operations across the Intelligence Community by creating a Human Intelligence Directorate outside the Directorate of Operations.

The new Act stipulates that the Director of the Central Intelligence Agency (DCIA) will "provide overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the Intelligence Community … and ensure that the most effective use is made of resources."[20] Consistent with this statutory mandate, we recommend the creation of a Human Intelligence Directorate—within the CIA

but separate from the existing Directorate of Operations—to serve as a national human intelligence authority, exercising the responsibility to ensure the coordination of all agencies conducting human intelligence operations on foreign soil.

The Human Intelligence Directorate would have direct "command" authority over CIA human intelligence components—which, if this Commission's recommendations are accepted, would be expanded to include not only the Directorate of Operations but also the proposed Innovation Center discussed in the following section. But its overseas human intelligence coordination responsibilities would extend more broadly across the Intelligence Community.

When most people think of human intelligence, they think about the CIA—and, more specifically, about the professional case officers in the CIA's Directorate of Operations (DO) who conduct the CIA's human espionage operations. But there are in fact a host of entities that collect human intelligence either through clandestine or overt means, ranging from long-established agencies like the Defense HUMINT service and the FBI to agencies that until recently had not viewed themselves as intelligence collectors (like immigration officials and customs officers). This range of entities conducting human intelligence activities, of course, raises serious coordination challenges—and these challenges are only becoming more formidable. As we discuss in Chapters Six (Management) and Ten (Intelligence at Home), both the Defense Department and the FBI are stepping up their own, more traditional overseas intelligence activities, as well as other, less conventional human intelligence efforts, such as those associated with the Department of Defense's special operations forces. While we believe that many of these efforts are commendable, they heighten the risk that intelligence operations will be insufficiently coordinated—a state of affairs that can, in the world of foreign espionage, have dangerous and even fatal consequences.

We propose the creation of the Human Intelligence Directorate within CIA to address this pressing need. The Directorate would coordinate the overseas operations of the DO with those of the Defense Department and the FBI. The CIA—with a network of case officers around the globe—is uniquely situated to perform this function, and its power to insist on such coordination should be reaffirmed. To accomplish this task, however, there are many issues the CIA's Human Intelligence Directorate will have to resolve with the Defense

Department and the FBI in establishing its authorities with respect to human intelligence. In order to ensure suitable attention to this process, we recommend the Director of CIA (DCIA) be required to report to the DNI, within 90 days of the DNI's confirmation, exactly what protocols have been established with the Defense Department and the FBI to ensure effective coordination among the three organizations and appropriate oversight of their respective activities.

The need for coordination is pressing and pronounced. Increasingly, for example, the FBI's intelligence operations cross national boundaries, thus requiring greater coordination with CIA and the Defense Department. The CIA, and in particular its field supervisors, should act as the focal point for overseas coordination to ensure that FBI tradecraft practices abroad reflect the hostile environment in which intelligence gathering occurs.

We emphasize three things that would *not* occur under our proposed system. First, other human intelligence collection agencies—to include DIA clandestine and overt operations, the Special Operations Command, and other human intelligence operations carried out by military services—would not surrender command authority and operational control over their human intelligence assets. Rather than "run" these components, the Human Intelligence Directorate would broadly direct and coordinate human intelligence activities overseas. Second, the DCIA's authorities as head of the Human Intelligence Directorate would not extend to directing collection against any specific target; rather, as discussed earlier in this Chapter and in Chapter Eight (Analysis), this responsibility would fall to Mission Managers. Third, we do not propose changing or stifling successful coordination efforts that already occur at "lower levels" in the field.

In addition to coordinating overseas human intelligence operations for the Community, the Human Intelligence Directorate would serve as the centerpiece for Community-wide human intelligence issues, including by helping to develop a national human intelligence strategy, integrating (where appropriate) collecting and reporting-disseminating systems, and establishing Community-wide standards for training and tradecraft. Finally, the Directorate also would have the responsibility for expanding, enriching, and diversifying the full range of human intelligence capabilities. We believe it is this task that makes it essential that the Human Intelligence Directorate be located within the CIA and under the direction of the Agency's Director—but *not* part of the

Directorate of Operations. As discussed in detail below, we believe that the DO is not ideally situated to incubate a variety of new human intelligence techniques, or to vet those developed by other agencies or entities, such as the Innovation Center.

Fostering Innovation

Recommendation 4

The CIA should develop and manage a range of new overt and covert human intelligence capabilities. In particular, a "Human Intelligence Innovation Center," independent of the CIA's Directorate of Operations, should be established to facilitate the development of new and innovative mechanisms for collecting human intelligence.

The Directorate of Operations, which conducts the CIA's human espionage operations, is one of the Intelligence Community's more elite and storied organizations. It takes justifiable pride in its ability to recruit spies and manage diplomatically delicate foreign liaison relationships. The DO has rigorous training programs—its premier training facility known colloquially as "the Farm," has become well-known through its depiction in popular movies and novels—and continues to attract some of the nation's most impressive talent.

It is a well-known rule of bureaucratic behavior, however, that when an organization does something particularly well, it is difficult to encourage that organization—or the people within it—to do things that are new and different.[21] And so it has proven with the Directorate of Operations. While the need to develop new methods of collecting human intelligence has been apparent for years, the DO has struggled to develop and "mainstream" new techniques, remaining wedded instead to the traditional model of recruiting spies.

We have seen positive indications that the new leadership of the CIA is aggressively exploring new human intelligence methods. If it is left to the DO to develop and implement these new ideas, however, we are skeptical that they will ever become more than a peripheral part of the DO's mission. Accordingly, we recommend the establishment of an "Innovation Center" within the CIA—but *not* within the Directorate of Operations—responsible for oversee-

ing the development of new and non-traditional methods of conducting human intelligence. This center's mission would be not only to evaluate and develop new human intelligence approaches, but also to serve as a think-tank and proving ground for new human intelligence techniques and methods. [22]

We recognize that there are arguments that such an innovation center should be placed outside of the CIA entirely, in light of the historically outsized influence that the DO has held over the CIA's management. But in our view it would be inadvisable to add yet another organization to the already dispersed constellation of human intelligence collection entities. (Indeed, as we suggested in the previous section, we believe that the CIA should exercise a *stronger* hand in coordinating human intelligence collection across the Intelligence Community.) The DNI, however, should monitor the Innovation Center closely, not only to ensure that it is performing its mission well but also to encourage the implementation of its useful new ideas.

In addition to this institutional recommendation to encourage the development of innovative new human intelligence practices, in our classified report we also point to several specific methods that in our judgment should either be explored or used more extensively. Unfortunately, these specific methods cannot be discussed in our unclassified report.

Professionalizing Human Intelligence Across the Community

We have been critical of the CIA's Directorate of Operations at certain points, but it is important also to emphasize what they do well. While we have concluded that the DO is not the best place to foster innovation in human intelligence, it does continue to set the standard for traditional human intelligence operational "tradecraft." It is to the DO that the rest of the Community should look for guidelines on asset validation and ways to build productive relationships with liaison services. We recommend that the DCIA, acting in his Community leadership role as the head of the Human Intelligence Directorate, work actively to develop and further professionalize human intelligence components outside of CIA in these and other areas.

For example, our review of the Community suggests that the Defense Department's attempts to develop a clandestine strategic intelligence arm have fallen short because of the absence of a professional human intelligence career path—for both military officers and civilians—and an overall environment that historically has not fostered sufficient respect for, or investment in,

human intelligence collection capabilities. While there are of course many talented Defense HUMINT clandestine case officers, the service has not developed the operational capability that it would possess if intelligence officers followed a long-term career path and passed on lessons learned.[23] We believe that the CIA—in its role as Community-wide human intelligence coordinator—should assist DIA in further professionalizing its cadre of clandestine case officers, and—in light of the Community-wide scarcity of fully-trained case officers—ensure that Defense HUMINT's clandestine service is properly leveraged and coordinated with the DO's operations.

Recommendation 5

The CIA should take the lead in systematizing and standardizing the Intelligence Community's asset validation procedures, and integrating them with all information gathering activities across the human intelligence spectrum.

The case of Curveball (described in detail in our Iraq study) illustrates the importance of integrating sound validation processes wherever possible—in all forms of human intelligence activities including unilateral collection, liaison-provided information, debriefings, and other human-acquired inputs into intelligence reporting. (By "validation processes" we mean the ways in which intelligence collectors ensure that the information provided to them is truthful and accurate.) The Pentagon's plans to increase its human intelligence capabilities make it especially important that Defense HUMINT adopt and institutionalize sound vetting and validation practices to ensure the reliability of information it disseminates to the Intelligence Community. It will be the responsibility of the Human Intelligence Directorate and the Defense Intelligence Agency to ensure that proper source validation occurs whenever possible, and that overt collectors are not simply passive conduits for human intelligence. In our classified report, we also make specific recommendations to improve the asset validation practices of human collection agencies that cannot be discussed in an unclassified format.

Collecting Human Intelligence: Custodial Interrogations

One source of critical intelligence, particularly with respect to terrorist plans and operations involving the use of nuclear, biological, or chemical weapons, is the interrogation of captured detainees. We consider it essential, and indeed have been assured that it is currently the case, that the Attorney General personally approves any interrogation techniques used by intelligence agencies that go beyond openly published U.S. government interrogation practices. While we recognize that public disclosure of Attorney General approved or forbidden techniques to be used by U.S. interrogators or by foreign personnel in interrogations in which the United States participates would be counterproductive, we emphasize that it is vital that all such practices conform to applicable laws. Where special practices are allowed in extraordinary cases of dire emergency, those procedures should require permission from sufficiently high-level officials to ensure compliance with overall guidelines, and records should be kept to provide oversight for deviation from regular practices. It is also important that notice of Attorney General approved techniques and the circumstances of any deviations from regular practices be given to appropriate congressional overseers. Interrogation guidelines should also form part of the training of relevant intelligence personnel. Compliance with approved practices should be uniformly enforced. Assurance that these steps have been taken across the Community will enhance the credibility of the Intelligence Community as a law-abiding and responsibly governed entity in the public mind, thereby enhancing its ability to perform its crucial functions.

Shaping the Force: A Larger and Better Trained Human Intelligence Officer Cadre

Recommendation 6

The Intelligence Community should train more human intelligence operators and collectors, and its training programs should be modified to support the full spectrum of human intelligence collection methods.

The reforms and initiatives discussed above would vastly improve our nation's human intelligence capabilities. But one thing will still be missing—the people necessary to do what needs to be done. We recognize the ease of saying "more money will solve the problem," and for that reason have avoided

recommendations that do little more than propose an outlay of additional funds. But in the case of human intelligence, we simply need more people.

In our classified report, we offer statistics showing how badly outgunned our human intelligence collectors are, at precisely the time when the most is expected of them. Although we make few recommendations that we believe will require substantial budget increases, we do believe that this is an area where increased funding for the purpose of expanding human intelligence forces would be appropriate—and where, as we have noted elsewhere (see Management, Chapter 6), the need for long term planning militates strongly toward a shift away from unpredictable supplemental budget appropriations. In our classified report, we offer additional recommendations on how to improve human intelligence training programs within the Intelligence Community. This discussion cannot be included in our unclassified report.

Technical Intelligence Collection

Signals and Imagery Intelligence

Signals intelligence and imagery collection systems are obviously critical to the Intelligence Community's ability to collect information. Unfortunately, as our Iraq case study vividly illustrates, a combination of factors—most relating to our adversaries' increasingly effective use of denial and deception—have significantly eroded the utility of the Community's legacy signals and imagery systems. In our classified report, we specify examples highlighting the scope of the problem.

The Community is investigating and developing numerous technologies and methods that can potentially surmount some of these collection challenges. These technologies cannot be discussed in detail in an unclassified report. However, we recommend that the DNI should, as an early priority, delve into the complex technical issues that surround these innovations. The DNI should also assist collectors in developing and operationalizing the most promising innovations, while redoubling efforts to improve *existing* means of countering and reducing the distorting effects of denial and deception.

To aid him in the latter effort, the DNI will inherit a commendable roadmap previously developed by the DCI. Among other things, this strategy establishes efforts to counter-denial and deception by our adversaries as "a top priority for the Intelligence Community."[24] Yet, like many DCI strategies, we are

concerned that the prose has not fully translated into practice. To ensure effective implementation, we suggest a mid-course review of the strategy's first five years: a thorough examination of accomplishments and shortfalls, an update of the principal actions that specific Intelligence Community entities have taken and should take, and a renewed effort to solicit the full backing and resources of relevant planning and acquisition professionals across the Community. The effort to overcome foreign denial and deception will be ongoing; there is no easy or quick fix for the problems that plague technical collectors.

In the short term, technical collectors' most important contributions to the Community's mission may occur when they operate in conjunction with other collection disciplines. As a result, we believe that implementation of the integrated collection enterprise we recommend in this chapter will significantly enhance the Community's ability to optimize its existing technical collection capabilities. Target Development Boards, in particular, will provide an ongoing opportunity to engage in cooperative collection efforts among collection disciplines—specifically to capitalize on the joint capabilities of technical and human collectors. Such joint activities have been at the source of some of the Community's most notable successes in recent years. In our classified report, we cite examples of types of joint efforts which we cannot discuss here.

Signals Intelligence in the United States

Recommendation 7

The President should seek to have the Foreign Intelligence Surveillance Act amended to extend the duration of electronic surveillance and "pen registers" in cases involving agents of foreign powers who are *not* U.S. persons.

The Foreign Intelligence Surveillance Act (FISA)[25] governs, in part, the manner in which the U.S. government may conduct electronic surveillance within the United States and electronic surveillance of U.S. persons abroad. NSA and the FBI have long operated within the confines of FISA and—according to NSA—the statute has not posed a serious obstacle to effective intelligence gathering. It has, however, become a growing administrative burden, because NSA (in cooperation with the FBI) must now obtain far more FISA warrants than it did when traditional communications were prevalent.[26]

The increased frequency with which NSA must obtain FISA orders, in turn, has placed a significant burden on the Department of Justice's Office of Intelligence Policy Review (OIPR), which represents the United States in the Foreign Intelligence Surveillance Court when NSA requires a FISA order.

We recommend that the President seek to have FISA amended to extend the duration of electronic surveillance and "pen register"[27] orders as they apply to agents of foreign powers who are *not* U.S. persons. We think the President might consider seeking an extension of the initial electronic surveillance period from 90 to 120 days, as well as an extension from 120 days to one year for follow-on orders. In addition, we recommend seeking an extension of the initial pen register period from 90 days to one year. Again, it is our view that each of these extensions should only apply to non-U.S. persons; by limiting the extension in this manner, the Justice Department and the FISA Court will maintain their current levels of attention when U.S. persons' civil liberties are implicated. Although these relatively modest changes to FISA procedures will not eliminate the burdens carried by NSA and the Department of Justice, we believe that they will at least lessen them and allow those agencies to focus their attention where it is most needed.

Measurement and Signature Intelligence

Recommendation 8

The DNI should appoint an authority responsible for managing and overseeing innovative technologies, including the use of technologies often referred to as "MASINT."

To its proponents, measurement and signature intelligence, or MASINT, is an unjustly overlooked specialty. A wide variety of collection techniques fall under the heading of MASINT—everything from sensors, lasers, ground-based radars, and pretty much any other technical measure that does not fit easily into the traditional intelligence disciplines.[28] Skeptics view these as a batch of unrelated technical intelligence tools, better developed and funded separately rather than under a single label.

Putting aside these definitional problems, some MASINT technical collection measures have had successes. Such technical capabilities can some-

times identify WMD programs, and can help counter denial and deception programs.

Although we are unsure of exactly how such techniques can best be supported, we are confident that the current situation is not the answer.[29] The designation of DIA—which lacks the staff, budget, and authority to control the development and deployment of MASINT systems—as the "National MASINT Manager" has failed to help these techniques prosper. These techniques are, almost by definition, some of the more innovative collection techniques in the Intelligence Community's arsenal, but they are often given short shrift as a result of DIA's neglect or disinterest.

We therefore recommend that the DNI take responsibility for coordinating new intelligence technologies, including those that now go under the title MASINT. This could be done by a special MASINT authority or as part of the DNI's Office of Science and Technology.

It is critical to note that, in our view, the MASINT coordinator should *not* directly control MASINT collection. Rather, we believe the most sensible division of MASINT responsibilities is that NGA be responsible for imagery-derived MASINT, while CIA and Defense Department elements take responsibility for their own operational sensors and other aspects of MASINT that fall naturally into their bailiwicks. At the same time, the DNI's designated representative would monitor the status of MASINT-like programs throughout the Intelligence Community to ensure that they are fully implemented and given the necessary attention.

Open Source Collection

Recommendation 9

The DNI should create an Open Source Directorate in the CIA to use the Internet and modern information processing tools to greatly enhance the availability of open source information to analysts, collectors, and users of intelligence.

Open Source information has long been viewed by many outside the Intelligence Community as essential to understanding foreign political, economic, social, and even military developments.[30] Currently, the Intelligence Commu-

nity has one collection organization, the Foreign Broadcast Information Service (FBIS), that specializes in providing some of these vital elements—particularly the rapid reporting of foreign print, radio, and television news. While this service is highly valued within the Community and academia, the Community does not have any broader program to gather and organize the wealth of global information generated each day and increasingly available, if only temporarily, over the Internet.

We also believe that the need for exploiting open source material is greater now than ever before. Today, the spread of information technology—and the ever increasing pace at which it advances—is immune to many traditional, clandestine methods of intelligence collection. Whereas advanced technological research once occurred only in large facilities and within enormous government bureaucratic institutions, today it can (and does) occur in nondescript office parks or garages, and with very small clusters of people. And for these new challenges, many open source materials may provide the critical and perhaps only window into activities that threaten the United States.

Much has happened in the world of open source in the past ten years. Internet search tools like Google have brought significant new capabilities and expectations for open source information to analysts and users alike. Regrettably, the Intelligence Community's open source programs have not expanded commensurate with either the increase in available information or with the growing importance of open source data to today's problems. This is an unacceptable state of affairs. Consider the following:

- ***The ever-shifting nature of our intelligence needs compels the Intelligence Community to quickly and easily understand a wide range of foreign countries and cultures.*** As we have discussed, today's threats are rapidly changing and geographically diffuse; it is a fact of life that an intelligence analyst may be forced to shift rapidly from one topic to the next. Increasingly, Intelligence Community professionals need to quickly assimilate social, economic, and cultural information about a country—information often detailed in open sources.

- ***Open source information provides a base for understanding classified materials.*** Despite large quantities of classified material produced by the Intelligence Community, the amount of classified information produced on any one topic can be quite limited, and may be taken out of

context if viewed only from a classified-source perspective. Perhaps the most important example today relates to terrorism, where open source information can fill gaps and create links that allow analysts to better understand fragmented intelligence, rumored terrorist plans, possible means of attack, and potential targets.

- ***Open source materials can protect sources and methods.*** Sometimes an intelligence judgment that is actually informed with sensitive, classified information can be defended on the basis of open source reporting. This can prove useful when policymakers need to explain policy decisions or communicate with foreign officials without compromising classified sources.

- ***Only open source can "store history."*** A robust open source program can, in effect, gather data to monitor the world's cultures and how they change with time. This is difficult, if not impossible, using the "snapshots" provided by classified collection methods.

We believe that this gap between the Intelligence Community's needs and its capabilities must be addressed on two fronts: collection and analysis. The former we discuss here; the latter is discussed more fully in Chapter Eight (Analysis).

We recommend that the DNI create an Open Source Directorate in the CIA to develop and utilize information processing tools to enhance the availability of open source information to analysts, collectors, and users of intelligence. At a minimum, such a program should gather and store many, if not most, of the digital newspapers and periodicals available over the Internet, regardless of language. (Daily storage is required because most of these newspapers and periodicals are on the Internet for only short periods of time.) We believe that this open source information will be invaluable to those charged with watching emerging threats and would provide a baseline for intelligence collectors and analysts when issues suddenly rise to national security significance. In addition, it can tip off analysts and collectors to changes that warrant more focused intelligence collection.

In the near term, we believe that without an institutional "champion" and home, open source will never be effectively used by the Intelligence Community. It is our hope that open source will become an integral part of all intelli-

gence activities and that, at some point in the future, there may no longer be a need for a separate directorate. We acknowledge that our recommendation could create one more collection specialty. But, for now, open source is inadequately used and appreciated and is in need of the high-level, focused attention that only a separate directorate can provide.

As important as collecting open source material, however, is the task of getting the material to the analysts who need it. We were repeatedly told that analysts have difficulty accessing open source information at their desks.[31] The Intelligence Community must make a concerted effort to solve the technology and security challenges associated with getting open source information to every analyst's desktop.

PROTECTING SOURCES AND METHODS

Our case studies strongly suggest that a persistent inability to protect human and technical collection sources and methods has substantially damaged U.S. intelligence capabilities. Authorized and unauthorized disclosures have compromised critical signals interception and satellite imagery programs, as well as hard-earned human intelligence sources. Better protection of these sources and methods, which should be thought of as the Community's crown jewels, will require sustained attention by the DNI and the consideration of a range of possible approaches. We believe that the act's emphasis on the DNI's obligation to protect sources and methods will help raise the priority placed on this important issue.[32] We also believe that the institutional recommendations in our information sharing chapter (Chapter 9)—which include making a single person in the office of the DNI responsible both for information sharing and for information security—will help ensure that information sharing imperatives do not overwhelm the need to protect sources and methods.

To accompany these institutional suggestions, we offer recommendations to help address two problems that have harmful effects on sources and methods: (1) the problem of *authorized* disclosures and (2) the problem of *unauthorized* disclosures (more commonly referred to as "leaks") of classified information.

Authorized Disclosures of Sources and Methods

Recommendation 10

Efforts should be taken to significantly reduce damaging losses in collection capability that result from *authorized* disclosures of classified information related to protection of sources and methods.

Authorized disclosures often have unintended and harmful effects. One common source of such disclosures is the sharing of intelligence with foreign countries both through cooperative ventures and diplomatic demarches. The Intelligence Community should take more rigorous steps to integrate counterintelligence expertise into the sharing and demarche decisions and processes, and to formally analyze the potential costs and benefits of such disclosures. These processes would need to include methods for tracking the consequences of unauthorized disclosures, and a formal process for resolving disputes among agencies and stakeholders over the costs and benefits of particular disclosure decisions.

Another *de facto* "disclosure" of information about the technical capabilities of intelligence satellites occurs when public announcements are made concerning a satellite launch. We therefore recommend that the United States examine whether its space launch techniques can be altered to shield spaceborne collection techniques and operations more effectively.

The Problem of Media Leaks

The scope of damage done to our collection capabilities from media disclosures of classified information is well documented. Hundreds of serious press leaks have significantly impaired U.S. capabilities against our hardest targets. In our classified report, we detail several leaks that have collectively cost the American people hundreds of millions of dollars, and have done grave harm to national security. We cannot, however, discuss them in an unclassified format. These and hundreds of other leaks have been reported to the Justice Department by the Intelligence Community in the last ten years. However, to date, not a single indictment or prosecution has resulted.

According to past government studies, the long-standing inability of the U.S. government to control press leaks results from a combination of fac-

tors—the use of unauthorized disclosures as a vehicle to influence policy, the lack of political will to deal firmly and consistently with government leakers in both the executive and legislative branches, the difficulty of prosecuting cases under existing statutes, and the challenge of identifying the leaker.[33] The government's impotence in dealing effectively with this problem was well characterized by then-Deputy Assistant Attorney General Richard K. Willard, in 1982:

> In summary, past experience with leaks investigations has been largely unsuccessful and uniformly frustrating for all concerned….The whole system has been so ineffectual as to perpetuate the notion that the Government can do nothing to stop the leaks.[34]

The Commission recognizes the enormous difficulty of this seemingly intractable problem and has considered a broad range of potential solutions. We conclude that the long-standing defeatism that has paralyzed action on this topic is understandable but unwarranted. Leaks cannot be stopped, but they can be reduced. And those responsible for the most damaging leaks can be held accountable if they can be identified and if the government is willing to prosecute them.

Recommendation 11

The DNI should ensure that all Inspectors General in the Intelligence Community are prepared to conduct leak investigations for their agencies; this responsibility can be coordinated by a Community-wide Inspector General in the Office of the DNI, if such an office is established.

Coordinated leaks investigations. The DNI Inspector General, assuming one is named, should be given specific responsibility for overseeing leaks investigations within the Intelligence Community and for coordinating investigations that require reaching into multiple agencies within the Community. The DNI's Inspector General would be uniquely positioned to coordinate leak investigations across the Intelligence Community. Several intelligence agencies have explained that the Justice Department is rarely willing to open investigations of leaks when the number of possible leakers is large. Furthermore, these agencies have expressed the opinion that complaining agencies should be allowed to conduct investigations of their own employees so as to

narrow down the list of possible leakers. By heeding these concerns, this recommendation will reduce the investigative load for the Justice Department and FBI while putting more of the burden on the agencies that often feel the impact of leaks most directly.

Vigorous application of DNI administrative authorities. When internal CIA leakers have been identified, the DCI's authority to impose sanctions ranging from fines, suspension or revocation of clearances, or even firings is relatively robust. This authority should extend to the DNI. The DNI should, in turn, vigorously enforce the 2002 DCI Directive on stemming unauthorized disclosures across the Community.[35] We hope that the 2002 Directive will acquire greater force under the new DNI than it has had under past DCIs.

Better education and training for intelligence producers, users, and media. Policymakers who leak intelligence to the press in order to gain political advantage and journalists who publish leaked intelligence may do so without fully appreciating the potential harm that can result to sources and methods. The Intelligence Community should consider implementing a widespread, modern-day equivalent of the "Loose Lips Sink Ships" campaign to educate individuals about their legal obligations—and possible penalties—to safeguard intelligence information. Officers at all agencies that produce and use intelligence should be fully briefed at the time they first sign the non-disclosure agreement and be periodically re-briefed about its responsibilities.

Internal changes at the Department of Justice. As noted more fully in Chapter Ten (Intelligence at Home), we recommend that the primary national security component of the Department of Justice be placed under the auspices of a single Assistant Attorney General. We do so in the hope that the combined forces of the Department can be better brought to bear on a variety of issues, including unauthorized disclosures.

Finally, there is one point regarding leaks on which the Commission could not come to agreement. During our work, we were repeatedly told that the greatest barrier to prosecuting leaks was in identifying the "leaker." And many people with whom we spoke also said that the best (if not only) way to identify leakers was through the reporters to whom classified information was leaked. In this vein, we thoroughly discussed the advantages and disadvantages of creating some sort of qualified privilege for reporters, which might simultaneously protect both First Amendment interests and the government's interest in protecting

classified information. Regrettably, and despite all of our efforts, we could not reach agreement on the details of such a proposal.

ENDNOTES

[1] Although the National Imagery and Mapping Agency (NIMA)—renamed the National Geospatial-Intelligence Agency (NGA)—was established after the Cold War, it was cast from the same mold.

[2] CIA, Title Classified (OTI IA 2002-141) (Aug. 26, 2002); CIA, Title Classified (OTI IA 2002-053 (SPS)) (Oct. 2004); CIA, Title Classified (OTI IA 2003-06) (Feb. 2003); Department of Defense Joint Staff, Title Classified (Dec. 2003); Defense Science Board, *Future Strategic Strike Systems* (Feb. 2004).

[3] National Intelligence Council (NIC), Title Classified (NIE 98-04) (1998-99).

[4] For a more detailed discussion of this issue, see Chapter Thirteen (Proliferation).

[5] NIC, Title Classified (NIE 98-04) (1998-90) at Volume 1.

[6] CIA, *The Jeremiah Report: The Intelligence Community's Performance on the Indian Nuclear Tests* (June 1, 1998) (hereinafter "Jeremiah Report").

[7] CIA, *Response to WMD Commission Request # 74* (Oct. 8, 2004).

[8] House Permanent Select Committee on Intelligence, IC21: *Intelligence Community in the 21st Century* (April 9, 1996) (hereinafter "IC21"); Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (1996) (hereinafter "Aspin-Brown Commission"); Jeremiah Report.

[9] *See, e.g.*, IC21.

[10] Target Development Boards would not just address analysts' needs. They would also address the needs of the military commanders for intelligence support to military operations.

[11] This idea is not unlike the Department of Defense's theory of Network Centric Warfare, which allows for widespread dissemination of data to the military to provide a shared awareness of the battle space. *See generally* Congressional Research Service, *Network Centric Warfare: Background and Oversight Issues for Congress* (June 2, 2004).

[12] Here we cite an example of an NSA acquisition problem that cannot be included in our unclassified report.

[13] Intelligence Reform and Terrorism Prevention Act of 2004 at § 1011, Pub. L. No. 108-458 (hereinafter "IRTPA").

[14] This includes the tactical programs in the Department of Defense. FY2005 NFIP, JMIP, and TIARA Congressional Budget Books.

[15] IRTPA at § 1011.

[16] We recognize that some competition in research and development is desirable and should be encouraged by the DNI. At the same time, even when research and development occurs in several locations, its efforts must still be integrated in a way that minimizes unproductive redundancy.

[17] *See, e.g.*, Memorandum from the President to the Director of Central Intelligence (Nov. 18, 2004).

[18] CIA, Directorate of Operations Recruitment (Sept. 14, 2004) (briefing slides).

[19] Interview with Defense HUMINT officials (Sept. 9, 2004).

[20] IRTPA at § 1011.

[21] *See generally* James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (Basic Books) (1989).

[22] If the innovation center proves a successful model, we believe the DNI should explore replicating it in other agencies as well.

[23] As we have already noted, we are far from the first to recognize the shortcomings in Defense HUMINT. *See, e.g.*, Aspin-Brown Commission; Council on Foreign Relations, *Making Intelligence Smarter: The Future of U.S. Intelligence* (1996); IC21; Defense Science Board *Task Force on Intelligence Support to the War on Terrorism* (Oct. 2003); House Permanent Select Committee on Intelligence, *Classified Annexes to The Intelligence Authorization Act For Fiscal Year 1998, 1999, 2003, 2004, 2005*.

[24] DCI, Title Classified (March 2000) at pp. 1-2.

[25] 50 U.S.C. §§ 1805, 1842.

[26] Interview with representatives of NSA's General Counsel's Office (Sept. 16, 2004); Interview with representatives of the Office of Intelligence Policy Review, Department of Justice (Oct. 25, 2004).

[27] A "pen register" or "trap and trace" device is roughly equivalent to using "caller identification" on a target phone (*i.e.*, it collects incoming and outgoing phone numbers).

[28] The term "MASINT" was first coined in 1970 by DIA to describe any number of disparate forms of collection and analysis such as active radar interrogation of targets, laser intelligence, optical measuring of reflected light from distant objects such as spacecraft, nuclear intelligence, acoustic intelligence, and infra-red analysis.

[29] According to DCI Porter Goss, "[p]ast efforts to manage MASINT have been hampered by an unrealistic view of MASINT as a single enterprise." Porter Goss, Director of Central Intelligence, *Cooperative Way Forward on MASINT Management* (Dec. 15, 2004) at p. 1.

[30] "Open Source" usually refers to all information that is generally publicly available and unclassified. It can include print media as well as radio and television broadcasting. With the advent of the Internet, there has been a major increase in the availability of open source textual data. This report focuses on, but is not limited to, this easily accessible open source textual data.

[31] *See, e.g.*, Interview with senior In-Q-Tel official (Feb. 3, 2005).

[32] The act states that the new DNI "shall protect intelligence sources and methods from unauthorized disclosure." It also limits the DNI's ability to delegate responsibility for protecting sources and methods, stating that the DNI "may only delegate" this authority to the Principal Deputy DNI. IRTPA at § 1011.

[33] National Counterintelligence Policy Board, *Report to the NSC on Unauthorized Media Leak Disclosures* (March 1996) at pp. C2-C4.

[34] *Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information* (March 31, 1982).

[35] DCI, Title Classified (Dec. 9, 2002).