CHAPTER EIGHT
ANALYSIS

Summary & Recommendations

The role of intelligence analysts is to tell policymakers what they know, what they don't know, what they think, and why. When analysts fail to provide adequate warnings of an impending threat, or provide incorrect conclusions to decisionmakers—as they did with Iraq—the consequences can be grave. Although there is no way to ensure against all future intelligence failures, we believe that several initiatives could improve management of analytic efforts, deepen analyst expertise, reduce intelligence gaps, and enhance the usability of existing information—all of which would improve the quality of intelligence.

Mission Managers, introduced in previous chapters, will play a critical role in this reform effort. They will encourage competitive analysis, present the views of all agencies to decisionmakers, ensure that analysts drive collection, and prepare the analytic community to meet the threats of the 21st Century.

In addition to adopting the Mission Manager approach, we also recommend—among other improvements—that the DNI:

- Emphasize strategic analysis by establishing a new long-term research and analysis unit, under the mantle of the National Intelligence Council, to serve as the lead organization for interagency projects involving in-depth analysis and expanded contacts with experts outside of the Intelligence Community;
- Institute Community-wide, career-long programs for training analysts and managers, and provide appropriate performance incentives;
- Develop and integrate into regular use new tools that can assist analysts in filtering the vast quantities of information that threaten to overwhelm the analytic process, as well as tools designed for foreign language exploitation; and
- Ensure that analysts are engaging in competitive analysis, mandate routine and ongoing examinations of finished intelligence, and require the lessons learned from "post mortems" to be incorporated into the intelligence education and training program.

INTRODUCTION

Analysts are the voice of the Intelligence Community.

While intelligence failures can certainly result from inadequate collection, recent experience shows that they can also occur when analysts don't effectively assess all relevant information and present it in a manner useful to decisionmakers. Improving the business of analysis should therefore be a major priority of the new Director of National Intelligence (DNI).

As in our chapter on collection, our recommendations—supported by vivid examples taken from our case studies—focus both on *integrating* analytical efforts across the Community and improving the overall *quality* of analysis.

The analytic effort in the Intelligence Community is hardly a monolithic enterprise; most of the Community's 15 organizations have at least one analytic component. Some of these agencies specialize in meeting the needs of particular users—notably the Defense Department's DIA and the State Department's INR. Some specialize in analyzing particular types of data—signals intelligence at NSA and geospatial intelligence at NGA. Some, such as the intelligence element of the Department of Energy, specialize in substantive intelligence topics, such as nuclear technology issues.

The separation of these analytic units serves a vital function; it fosters competitive analysis, encourages a diversity of viewpoints, and develops groups of analysts with different specialties. Any reform of the Community must preserve these advantages; our suggested move toward greater integration should not mean the homogenization of different viewpoints. Nevertheless, there is a great and growing need for Community analytic standards, interoperable and innovative technologies, access to shared information, and a common sense of mission. In many cases today, analysts in the 15 organizations are unaware of similar work being done in other agencies. Although analysts may develop working relationships with counterparts in other organizations, there is no formalized process or forum through which to do so. These dysfunctional characteristics of the current system must change; collaboration must replace fragmentation as the analytic community's primary characteristic.

Despite the fact that the analytic units are largely isolated and autonomous, we have been deeply impressed by pockets of excellence within them. The

Community is blessed with a highly intelligent, dedicated analytic workforce that has achieved significant successes. We also note that, in response to Iraq-related failures, the Intelligence Community has recently undertaken several serious (although scattered) efforts to improve the overall quality and integrity of its analytical methods and products.

We conclude, however, that these strengths and reforms are too few and far between. Our investigation revealed serious shortcomings; specifically, we found inadequate Intelligence Community collaboration and cooperation, analysts who do not understand collection, too much focus on current intelligence, inadequate systematic use of outside experts and open source information, a shortage of analysts with scientific and technical expertise, and poor capabilities to exploit fully the available data. Perhaps most troubling, we found an Intelligence Community in which analysts have a difficult time stating their assumptions up front, explicitly explaining their logic, and, in the end, identifying unambiguously for policymakers what they *do not know.* In sum, we found that many of the most basic processes and functions for producing accurate and reliable intelligence are broken or underutilized.

This Commission is not the first to recognize these shortcomings—we trod a well-worn path. Again and again, many of the same obstacles to delivering the best possible analytic products have been identified. The Church Committee's 1976 report, the House Permanent Select Committee on Intelligence's 1996 study of the Intelligence Community in the 21st Century, the 1998 Rumsfeld Report side letter to the President, the 1999 Jeremiah Report, the Markle Foundation's 2003 Task Force, and the 9/11 Commission Report all pointed to the problems created by the poor coordination and resistance to information sharing among Intelligence Community agencies. Some studies, notably the 1996 report by the Council on Foreign Relations and the 1996 study by the Aspin-Brown Commission, noted the need to systematically engage in and use competitive analysis. As early as 1949, the Hoover Commission faulted the Intelligence Community for failing to improve relations with decision-makers, and these concerns were echoed by the Aspin-Brown Commission and, most recently, the Markle Foundation Task Force.[1] Finally, the House and Senate intelligence committees have both noted the problems the Intelligence Community faces in processing the collected information available to it, as well as the difficulty analysts have engaging in long-term analysis, given the press of daily demands.[2]

In other words, many of the problems we have identified have been apparent to observers of the Intelligence Community—and to the Community itself—for decades. Nevertheless, they have remained largely unresolved, due largely to institutional resistance to change, the classified nature of the work, and a lack of political will to enforce change.

We believe the creation of the Office of the DNI offers a unique opportunity to finally resolve many of these issues by infusing the analytic culture with new processes and Community standards. We believe that this new management structure can foster a new sense of community among analysts. Until the analytic community adopts a new approach, analysts at one agency will continue to be denied access to critical reporting from others; analysts will resist collaborating and coordinating across units; managers will persist in placing the need to answer the "daily mail" over the need to develop true expertise; and new commissions will be appointed in the wake of future intelligence failures. As discussed in previous chapters, we believe that the creation of Mission Managers will be an important factor in avoiding this grim outcome.

Our recommendations, therefore, focus on exploiting the opportunity presented by the new legislation and the creation of the Office of the DNI, as well as on instituting changes to the Community's culture that will improve analytic performance. In doing so, we offer specific suggestions for how the community of analysts can be better integrated without sacrificing all-important independent analysis, and how the Intelligence Community can ensure that analysts have the tools, training, and "tradecraft" practices to ensure that the analytic community is prepared to meet today's and tomorrow's threats.

Achieving Community Integration Among Analysts

We believe that a principal goal of improving analysis should be to integrate the community of analysts while at the same time promoting independent—or competitive—analysis. In this sense, we believe a major challenge for the first Director of National Intelligence will be to foster more collaboration among analysts across the Community—that is, to bring the benefits of collaboration to daily support to the President, to strategic intelligence and warning, and to assistance to military, law enforcement, and homeland security efforts. In our view, there are five prerequisites to creating such a community:

Achieving Community Integration Among Analysts (Continued)

- ***Community standards*** for analysis (analytic expertise, analytic performance, and analytic presentation to consumers) so that the work of any one analytic unit can be relied upon and understood by others;
- ***A common analytic work environment*** (a shared network, compatible tools, and a common filing system for products and work in progress) so that a DNI can know the state of intelligence on critical issues, and so knowledge and supporting data can be shared quickly and efficiently across the Community;
- ***A group of "Mission Managers,"*** acting on behalf of the DNI, to oversee the state of intelligence on designated priority issues (including the state of analytic skills and resources, the gaps in existing knowledge, strategies to fill those gaps, and the effectiveness of agreed upon collection strategies)—from a Community perspective;
- ***A body of "joint" analysts*** to work in concert with analysts across the Community—to help fill gaps in strategic research as distinct from current reporting, to prompt collaboration on tasks that merit a Community perspective, and to help spread sound analytic methods and standards; and
- ***Daily intelligence support to the President***, without which the DNI would find it very hard to impose standards and priorities on organizations free to plead the exigencies of meeting immediate needs of important clients.

MANAGING THE COMMUNITY OF ANALYSTS

As we have discussed in our chapters on management and on collection, no single individual or office in today's Intelligence Community is responsible for getting the answers right on the most pressing intelligence issues of our day. We have recommended the creation of Mission Managers to fill this role, and they will perform a variety of essential tasks—including leading the development and management of collection strategies against high-priority intelligence targets. Because we believe that analysis must drive the collection process, it will be vital that Mission Managers also act as leaders in the analytic community. First and foremost, they must assess the strengths and weaknesses of analytic production in their areas of substantive responsibility.

These assessments will enable Mission Managers to develop strategic analysis plans to guide the Community's analytic efforts over the long term. Moreover, the assessments will guide Mission Managers in their role as chairs of Target Development Boards; their understanding of the gaps in analysts' knowledge will ensure that these gaps do in fact drive collection.

Armed with a clear understanding of where expertise resides in the Community, Mission Managers will also be able to foster competitive analysis. We expect that Mission Managers will ensure that finished intelligence routinely reflects the knowledge and competing views of analysts from all agencies in the Community. In particular, we expect that Mission Managers will encourage analysts to make differences in judgments, and the substantive bases for these differences, explicit in all finished products.

Recommendation 1

Mission Managers should be the DNI's designees for ensuring that the analytic community adequately addresses key intelligence needs on high priority topics.

To accomplish this, Mission Managers must have a comprehensive view of the skills and knowledge of the Community as a whole. The DNI should call on all agencies to provide—and regularly update—information about the knowledge and skills of their analysts, including their academic backgrounds, professional experiences, military experiences, and languages. The DNI's staff should make this information accessible through an easy-to-use directory and search tool. Mission Managers and agency heads would draw on this information to identify existing gaps, develop strategies to fill them, and create long-run strategic plans to avoid gaps on critical intelligence issues.

The model we envision is in stark contrast to the status quo, in which decisionmakers and analysts have little ability to find, track, and allocate analytic expertise. Although some efforts have been made to create such a database, ironically organizations have contributed information on the condition that other agencies not have access to their data. Our interactions with various agencies strongly suggest that the Intelligence Community still lacks a full understanding of the number, type, and skill-level of analysts in the various analytic organizations.[3] Therefore it is difficult to identify the

gaps in expertise for purposes of hiring, training, supervising professional development, or managing day-to-day work. Today, line managers identify the gaps in expertise in their own analytic organizations, but little is done to understand gaps from the perspective of an entire agency, much less the entire Community. With so weak a grasp of the Community's analytic resources, it is no wonder that agencies have difficulty quickly aligning their resources to respond to crises.

Even in the area of counterterrorism, which has consistently received high-level attention, agencies have struggled to establish a true Community analytic counterterrorism effort. The only way the Intelligence Community could bring together counterterrorism analytic expertise was to pull analysts away from their home agencies and house them together. From its inception, the Terrorist Threat Integration Center (now NCTC) faced fierce bureaucratic resistance in its efforts to do just this.

We believe a Mission Manager could respond to this or similar challenges more intelligently, quickly, and decisively. A Mission Manager would be able to (1) identify where analytic expertise resided and call on analysts from a variety of agencies to respond to critical questions; (2) identify and recommend to the DNI which analysts should be moved within or between agencies, if required in order to respond to a crisis; (3) "surge" on such a crisis, in the event that Community resources were insufficient, by tapping outside experts to contribute their expertise; (4) create a "virtual center" without physically co-locating analysts and without establishing a segregated and centrally-managed body to analyze a particular subject matter; and (5) clearly define organizational roles rather than letting bureaucratic dogfights, such as those surrounding TTIC, determine who has responsibility for which task. This, we believe, is how the analytical community should be managed.

Although Mission Managers would manage analysis by substantive area, they would not—in contrast to a center like the National Counterterrorism Center or the National Intelligence Council—actually *do* extensive intelligence analysis. Rather, a Mission Manager should coordinate and oversee decentralized analysis. By maintaining this separation of responsibilities, we believe that Mission Managers can prevent so-called "groupthink" among analysts. Indeed, we think fostering competitive analysis within the Community is a critical aspect of the Mission Manager's role.

We acknowledge that the Mission Managers will, if effective, interfere with the current autonomous management of analytic resources within individual organizations. But we see this as a strength, ensuring that members of the Community work together instead of at odds with one another. The risk, of course, is that a Mission Manager with a strong analytic viewpoint could reduce, rather than foster, competitive analysis. While this may sometimes happen—because Mission Managers must have substantive expertise to guide the Community's work—we expect Mission Managers to act more as facilitators of analytic products than as senior analysts. Consequently, their role most often should be to clearly present analytic viewpoints—including alternative views—to policymakers. If a Mission Manager fundamentally disagrees with the prevailing view in the Community, the Mission Manager could present his own view as an alternative, but he should not silence the perspective of other specialists in the Community.

Although not a precondition for success, our vision for Mission Managers ultimately requires a significant technological change—the creation of a "common work environment" for the community of analysts working on a topic. By "common work environment" we mean a shared information network with compatible computer tools and a common computer filing system for analytic products. Such technology is necessary to permit the Mission Manager to have full visibility into the emerging analytic work that is (or is not) being done on a topic, the basis for analytic assessments, and the degree of collaborative involvement between analysts and collectors. This common work environment will also enable greater collaboration between analysts in different agencies, as well as with the nucleus of analysts we recommend placing in the National Intelligence Council (see below).

A final note about managing the Intelligence Community's analysts: we recommend that one of the DNI's earliest undertakings be to have a senior advisor assess the Intelligence Community's medium- and long-term analytic needs, identify analytic gaps, and recommend ways to fill those gaps. And because the Intelligence Community's needs should be closely correlated with policymaker priorities, policymakers should be included in this assessment. Recommendations for correcting deficiencies might include such methods as targeted hiring, correcting national educational shortcomings, or contracting with outside experts.

TAPPING NON-TRADITIONAL SOURCES OF INFORMATION

Analysts have large quantities of information from a wide variety of sources delivered to their desktops each day. Given the time constraints analysts face, it is understandable that their daily work focuses on using what's readily available—usually classified material. Clandestine sources, however, constitute only a tiny sliver of the information available on many topics of interest to the Intelligence Community. Other sources, such as traditional media, the Internet, and individuals in academia, nongovernmental organizations, and business, offer vast intelligence possibilities. Regrettably, all too frequently these "nonsecret" sources are undervalued and underused by the Intelligence Community. To be true all-source analysts, however, Community analysts must broaden their information horizons. We encourage analysts to expand their use of open source materials, outside experts, and new and emerging technologies.

To facilitate analysts' productive use of open source information, the Intelligence Community should create an organization responsible for the collection of open source information. We discuss the need for an open source organization in greater detail in Chapter Seven (Collection). It merits emphasis here, however, that simply creating this organization is unlikely to be sufficient. Analysts who routinely receive clandestine reporting too often see unclassified reporting as less important, and they spend too little time reviewing and integrating data available through open sources. Analysts on lower priority accounts use open source materials because they have difficulty getting clandestine collectors to assist them, but even they receive little or no training on how to evaluate available open sources or find the best information most efficiently.

Recommendation 2

The DNI should create a small cadre of all-source analysts—perhaps 50—who would be experts in finding and using unclassified, open source information.

As the CIA increases its analytic workforce, a small number could be reserved and trained specifically in open source research. They could then be assigned to offices willing to experiment with greater use of open source

material, where they would be expected to answer questions for and provide useful unclassified information to analysts. They would also produce their own pieces highlighting open source reporting but drawing on classified information as well.[4] We see these "evange-analysts" as essentially leading by example. They should show other analysts how to find and procure useful open source material, how to assess its reliability and biases, and how to use it to complement clandestine reporting.

We acknowledge that, given the demand for more analysts, there are real costs to designating even this small number as open source specialists. But we expect that the need for these specialized analysts will not be permanent. Over time, the knowledge this group has about open sources is likely to be absorbed by the general population of analysts—as a result both of their education outreach efforts and of the influx of younger, more technologically savvy analysts. As this happens, these open source specialists can be absorbed into the broader analytic corps.

In addition to this special cadre of analysts, the Community will need to find new ways to deal with the challenges presented by the growing availability of open source materials. Among these challenges is the critical problem of processing increasing numbers of foreign language documents.

Recommendation 3

The DNI should establish a program office within the CIA's Open Source Directorate to acquire, or develop when necessary, information technologies to permit prioritization and exploitation of large volumes of textual data without the need for prior human translation or transcription.

Information technology has made remarkable advances in recent years. The private sector (without the same kinds of security concerns as the Intelligence Community) has led the adoption of technologies that are also critical to intelligence. Two areas show particular promise: first, machine translation of foreign languages; and second, tools designed to prioritize documents in their native language without the need for translation.

The Community will never be able to hire enough linguists to meet its needs. It is difficult for the Community to predict which languages will be most in

demand and to hire the necessary linguists in advance. And even an aggressive hiring and training effort would not produce an analytic workforce that can absorb the huge quantity of unclassified foreign language material available today.

Eventually, all analysts should have basic foreign-language processing tools easily available to them so that even those who are not language-qualified can pull pieces of interest and get a quick, rough translation. NSA has done pioneering work on machine translation and is pursuing a number of separate initiatives; the military services, CIA (including In-Q-Tel), and other agencies sponsor largely independent projects. There is an abundance of activity, but not a concerted, coherent effort, which has led to steady but slow development.

Advanced search and knowledge extraction technologies could prove to be even more valuable than machine translation (and of course, the two are very much related). We refer here to software that uses mathematical operations, statistical computations, and relational analyses to cluster documents and other data by subject, emphasis, and association in order to identify documents that are similar even when the documents do not use the same key words. Other types of software algorithms can discern concepts within a text; some can depict relationships between ideas or between factual statements based on an understanding of the word's meaning rather than merely searching for a word verbatim. As these tools mature, they will be invaluable to agencies that now find themselves collecting more information than they can analyze. They will also become essential to analysts caught in a similar avalanche of data.

The Intelligence Community has only begun to explore and exploit the power of these emerging technologies. The Intelligence Community's current efforts should be coordinated, consolidated where appropriate, directed, and augmented. Therefore, we suggest that the DNI establish a program office that can lead the Community effort to obtain advanced information technology for purposes of machine translation, advanced search, knowledge extraction, and similar automated support to analysis. This office would draw on the various initiatives in these areas dispersed throughout the Intelligence Community. It would work to avoid duplication of effort and would promote collaboration and cross-pollination. It would serve as a knowledge bank of state-of-the-art technology. It would also serve as a testbed, using open source information to

experiment with software that has not yet been certified for classified environments. When appropriate, it would hand off successful technologies for use on classified networks. While we would place the program office in the new Open Source Directorate, where quick deployment seems most likely to occur, we recognize that NSA is a center of excellence for linguistics and technology, and it must surf a data avalanche every day. For that reason, we suggest that the program office be jointly staffed by NSA and CIA.

Context Is Critical

Many of the intelligence challenges of today and tomorrow will, like terrorism or proliferation, be transnational and driven by non-state actors. Analysts who cover these issues will need to know far more than the inclinations of a handful of senior government officials; they will need a deep understanding of the trends and shifts in local political views, cultural norms, and economic demands. For example, analysts seeking to identify geographic areas likely to be receptive to messages of violence toward the United States will need to be able to distinguish such areas from those that, while espousing anti-U.S. rhetoric or advocating policies at odds with the interests of the United States, nevertheless eschew violent tactics.

Clandestine collectors, however, are poorly structured to fill the intelligence gaps these analysts face. Imagery is of little utility, and both signals and human intelligence are better positioned to provide insight into the plans and intentions of a few important individuals rather than broader political and societal trends.

As a result, analysts are supplementing clandestine collection not only with a greater reliance on open source material and outside experts, but also with their own expertise. To enable them to do so, the Intelligence Community must expand analysts' opportunities to travel and live overseas. And it must consider reforms to the security clearance process that often hampers recruitment of those with the most experience living and working among groups of interest to the Community. Failure to think creatively about how to develop an analytic cadre with a deep understanding of cultures very different from our own will seriously undermine the Community's ability to respond to the new and different intelligence challenges of the 21st century.

Recommendation 4

The Intelligence Community should expand its contacts with those outside the realm of intelligence by creating at least one not-for-profit "sponsored research institute."

We envision the establishment of at least one not-for-profit "sponsored research institute" to serve as a critical window into outside expertise for the Intelligence Community. This sponsored research institute would be funded by the Intelligence Community, but would be largely independent of Community management. The institute would both conduct its own research as well as reach out to specialists, including academics and technical experts, business and industry leaders, and representatives from the nonprofit sector and from Federally Funded Research and Development Centers.

Free from the demands created by the events of the day that burden those within the Intelligence Community, this sponsored research institute's primary purpose would be to focus on strategic issues. It would also serve as an avenue for a robust, external alternative analysis program. Whatever alternative analysis the Community undertakes internally—and we see this as essential—there must be outside thinking to challenge conventional wisdom, and this institute would provide both the distance from and the link to the Intelligence Community to provide a useful counterpoint to accepted views. In this vein, the DNI might consider establishing more than one such institute. By doing so, competitive analysis would be further promoted and healthy competition between the research institutes would help both from being co-opted by the Intelligence Community.

This sponsored research institute would eliminate some existing impediments to more extensive outreach. The institute would have a budget that would enable it to pay top experts unwilling to work for the lower rates typically offered by Intelligence Community components. Moreover, contractors linked to the institute would be available to all Intelligence Community components, avoiding any suggestion that contractors were tasked to provide assessments to support the views of a particular agency. Further, although the staff of the research institute would take recommendations from analysts for particular people to contact outside of the Community, we expect the staff itself to pull together possible contacts in critical fields, expanding the circle

of those whose knowledge would be available to the Intelligence Community. The sponsored research institute could also become a center for funding non-traditional methods of assembling open source information. In our classified report we provide an example that cannot be discussed in an unclassified format.

Such a sponsored research institute is not the only way to capitalize on expertise from outside the Intelligence Community. Although the institute would expand the Community's ongoing outreach efforts, the Intelligence Community also needs to think more creatively and, above all, more *strategically* about how it taps into external sources of knowledge. This may include recognizing that the Community may simply not be the natural home for real expertise on certain topics. While economic analysts, for example, can and do play a valuable role in the Community, economists at the Federal Reserve, World Bank, or private sector companies investing millions in emerging markets are likely to have a better handle on current market conditions. Relying on these experts might free up Community resources to work more intensely on finding answers no one else has.

Each of these proposals assumes the Community will have access to existing experts, but that will not always be the case. As a result, the Community must also find ways to support the development of the external expertise it needs. One biosecurity expert remarked that what we really need is a major effort to foster publicly-minded experts to tackle the biothreats likely to face the United States in the future.[5] Title VI of the Higher Education Act, which supports language and area studies in universities, and the National Security Education Program (the Boren Program) might also help. We believe the Intelligence Community should think even more broadly about ways to meet national information needs.

Finally, analysts also need to take full advantage of currently available and underutilized non-traditional technical intelligence capabilities, like advanced geospatial intelligence techniques and measurement and signature intelligence (MASINT). Analysts would benefit from additional training and education to increase their awareness of new and developing collection techniques, so that they are able to effectively task these sources and use the information provided.

MANAGING THE INFLUX OF INFORMATION

As countless groups both inside and outside the Intelligence Community have commented, there is a dire need for greater information sharing—or, as we prefer to put it, information *access* in the Intelligence Community. We address this topic more fully in Chapter Nine (Information Sharing).

But analysts not only need more information, they also need new ways to manage what is already available to them. Analysts today "are inundated and overloaded with information."[6] A study published in 1994 revealed that analysts on average had to scan 200 to 300 documents in two hours each day, just to discover reports worth writing about.[7] If we assume that relevant information has doubled for most analytic accounts over the past ten years (a gross understatement if open source information is considered)—and if we depend on analysts not just to pick reports to write about but instead to "connect the dots" among names, phone numbers, organizations, and events found in other documents—the typical analyst would need a full workday just to perform the basic function of monitoring new data.

The private sector is already using tools and techniques to handle the greatly increased flow of information in today's world; many of the best of these operate even before a user begins to look for relevant information. By the time an Internet user types search terms into Google, for example, the search engine has already done a huge portion of the work of indexing the information and sorting it by relevance. In fact, Google already has educated guesses about what information will be most useful regardless of the breadth of the user's search.

The Intelligence Community's widely used tools for processing raw intelligence traffic are far weaker. According to a senior official at CIA's In-Q-Tel, when analysts enter the Intelligence Community they discover that they have "left a world that was totally wired."[8] Today, an analyst looking for information on Intelligence Community computers is effectively performing a keyword search without any relevance ranking or additional context. The Community has been largely resistant to efforts to import tools from the private sector that offer new and different ways of using technology to exploit data.[9] While this resistance is often driven by legitimate concerns about security, these concerns can (and must) be overcome in the development of information technology for the Intelligence Community.

Recommendation 5

The Community must develop and integrate into regular use new tools that can assist analysts in filtering and correlating the vast quantities of information that threaten to overwhelm the analytic process. Moreover, data from all sources of information should be processed and correlated Community-wide *before* being conveyed to analysts.

The Intelligence Community is only in the beginning stages of developing effective selection, filtering, and correlation tools for its analysts, and more progress must be made. While in every case people are needed to see whether the proposed connections are real—and to be alert for intuitive but inchoate linkages—the Intelligence Community must more effectively employ technology to help draw attention to connections analysts might otherwise miss.

But better tools are not the whole answer. Time and again, tools introduced to the Intelligence Community have failed to take hold because the Community's analysts were accustomed to doing business a different way. We therefore believe there is a need to improve on the Community's long standing, but now outdated, basic approach to processing, exploiting, and disseminating information. In our view, the Intelligence Community needs processes that help analysts correlate and search large volumes of data after traditional dissemination by collectors but *before* the information overflows analysts' inboxes.

Without such a change, we are afraid that analysts will be overwhelmed by piles of information through which they have little hope of sorting.

FOSTERING LONG-TERM RESEARCH AND STRATEGIC THINKING

Managers and analysts throughout the Intelligence Community have repeatedly expressed frustration with their inability to carve out time for long-term research and thinking. This problem is reinforced by the current system of incentives for analysts, in which analysts are often rewarded for the number of pieces they produce, rather than the substantive depth or quality of their production.

Analysts are consistently pressed to produce more pieces faster, particularly those for current intelligence publications such as the President's Daily Brief (PDB). One analyst told us that if an office doesn't produce for the PDB, its "cupboard is bare."[10] But constant pressure to write makes it hard for analysts to find time to do the research—and thinking—necessary to build the real expertise that underlies effective analysis. In one particularly alarming example, an Iraq analyst related that the demand for current intelligence became so acute that he not only gave up long-term research, but also stopped reading his daily in-box of intelligence reporting. That task was delegated to a junior analyst with no expertise on Iraq weapons of mass destruction issues who pulled traffic he thought might be of interest.[11] Although this is an unusually dramatic example, we provide additional classified statistics illustrating this problem in our classified report.

The drive to fill current publications can also crowd out work on strategic military and proliferation issues. As with long-term research, work on these issues may fall by the wayside as analysts respond to immediate, tactical policymaker interests. And strategic work may be discouraged simply because presenting it in a format usable by current intelligence publications is difficult or impossible. Technical assessments are generally seen as too cumbersome for daily intelligence and more difficult for the non-technical briefers to discuss should the President choose to have a dialogue on the issue. Although some of these products reach senior policymakers separately, the fact that they are typically excluded from the publication designed to inform the President about the most important issues of the day likely suggests to analysts that this work is not as highly valued as other topics.

Managers with whom we spoke are aware of the dearth of strategic, long-term thinking, and are seeking ways to remedy the problem. However, we think that part of the solution lies within the new office of the DNI.

Recommendation 6

A new long-term research and analysis unit, under the mantle of the National Intelligence Council, should wall off all-source analysts from the press of daily demands and serve as the lead organization for interagency projects involving in-depth analysis.

We recommend placing this new unit under the National Intelligence Council where analysts would be able to focus on long-term research and underserved strategic threats, away from the demands of current intelligence production. Although some analysts in this new organization would be permanently assigned, at least half—and perhaps a majority—would serve only temporarily and would come from all intelligence agencies, including those with more specialized analysts, such as NGA and NSA. Typically, analysts would have two-year assignments in the unit; in some cases, analysts may spend shorter periods in the organization, long enough to complete a single in-depth research project of pressing need. Because we expect the topics tackled by this group to be complex, collaboration with those outside the unit should be pervasive.

We envision the analysts located in this unit leading projects that bring in experts from across the Intelligence Community, as well as from outside the sphere of intelligence. This collaboration will enable the Intelligence Community to tackle broad strategic questions that sometimes get missed as many analysts focus on narrow slivers of larger issues. DIA analysts and managers, for example, told us that the current division of key analytical responsibilities among the various Department of Defense intelligence units at DIA, the service intelligence centers, and the unified commands makes it difficult for DIA to develop an integrated, strategic assessment of emerging security issues. We expect this new organization to fill such gaps.

Some might be concerned that this new analytic unit would create unhealthy barriers between those engaged in current intelligence and those conducting long-term research. But as proposed, this office avoids that division. Using the common technology infrastructure we propose, we expect that analysts in the new office would easily be able to draw on the insight of analysts still in their home offices who are working on current intelligence. Moreover, because analysts would rotate through this office and remain only for a short period of time, they would not run the risk of veering off into studying questions that might be intellectually interesting but are unlikely to be important to decision-makers. These analysts would come to the office with an understanding of the pulse of current intelligence. Even more important, those same analysts would return to their line units, and the production of timely intelligence, with a greater depth of understanding of their accounts.

Rotations to this unit would also reinforce habits that should be second nature, but sometimes get lost in the daily press of business. Analysts would have time to think more carefully about their words, ensuring that terms used to express uncertainty or concerns about credibility were consistent over time and across accounts. We hope that this unit would also engage in alternative analysis—and that this would help to foster alternative analysis throughout the Intelligence Community. Moreover, rotations through this unit would foster a greater sense of community among analysts and spur collaboration on other projects as well.

Although this strategic analytic unit could be housed in a number of places, we believe that the NIC is best. First, the NIC remains today one of the few places within the Intelligence Community that focuses primarily on long-term, strategic thinking. Second, the NIC is already accustomed to working with analysts across the Community and is therefore likely to be seen as an honest broker—an organization that treats analysts from different agencies equally. Third, the NIC already regularly engages outside experts. Indeed, many National Intelligence Officers spend the bulk of their careers outside the intelligence field.

ENCOURAGING DIVERSE AND INDEPENDENT ANALYSIS

Throughout our case studies we observed the importance of analysts clearly identifying and stating the basis for their assessments. But good analysis goes well beyond just saying what is known, what is unknown, and what an analyst thinks. It is critical that analysts find ways of routinely challenging their initial assumptions and questioning their conclusions—in short, of engaging in competitive (or, as we prefer to call it, independent) analysis.

Recommendation 7

The DNI should encourage diverse and independent analysis throughout the Intelligence Community by encouraging alternative hypothesis generation as part of the analytic process and by forming offices dedicated to independent analysis.

We believe that diverse and independent analysis should come from many sources. In this vein we offer several recommendations that should foster diverse and independent analysis, most particularly our proposed long-term research and analysis unit in the National Intelligence Council, our proposed not-for-profit sponsored research institute, the preservation of dispersed analytic resources, and Community training that instills the importance of independent analysis.

To begin, we note ongoing efforts within the Intelligence Community that have provided valuable independent analysis. The CIA's Directorate of Intelligence, for example, currently has an organization that exclusively drafts "red cell" pieces—documents that are speculative in nature and sometimes take a position at odds with the conventional wisdom.[12] This office proved especially valuable in the context of Libya, for reasons we discuss in greater detail in our classified report but cannot discuss here.

We foresee our proposed long-term research and analysis unit augmenting such existing efforts. We envision the office conducting some of its own alternative analysis, working with analysts in their home offices to conduct independent analysis, and ensuring that analytic judgments are routinely challenged as new information becomes available. By both engaging in its own work and working in conjunction with other offices, we hope that the unit will help catalyze independent analysis throughout the Community and, in the long run, ensure that independent analysis becomes part of the standard way of thinking for all analysts.

Our envisioned not-for-profit sponsored research institute is another natural location for independent analysis to be conducted. In fact, a well-designed research institute should be ideal in that it would have close relationships with non-Intelligence Community experts, as well as easy access to large volumes of open source material. Similarly, the National Intelligence Council should further foster alternative analysis through a National Intelligence Estimate (NIE) process that promotes dissenting views. In our view, the NIE process today is designed to serve as a Community product and, as such, can sometimes become a consensus building process. We hope that the DNI will encourage the NIE drafters to highlight and explore dissenting opinions.

We must stress, however, the importance of fostering a culture of alternative analysis *throughout* the Intelligence Community, as opposed to centralizing

the function in a single office (or even several offices). An office solely responsible for dissenting opinions is at risk of losing credibility over time, which would not make it an attractive place for analysts to work. Moreover, we are afraid that an office dedicated to independent analysis would—in the long run—end up having its own biases, and would not provide the diversity of views that we think is so important.

We thus recommend that the DNI give particular "red-team" or "devil's advocate" assignments to individuals or offices on a case-by-case basis, rather than trying to produce all alternative analysis through a separate office. By doing so, no individual or office would constantly bear the brunt of criticizing other analysts' work, nor would such alternative analysis be thought to be the sole responsibility of a single, stand-alone office. And while the DNI is statutorily required to assign an individual or entity responsibility for ensuring that the Community engages in alternative analysis,[13] this should not in our view artificially limit the locations in which such analysis occurs.

Perhaps most important, however, is the view that the Intelligence Community should not rely upon specialized "red team offices," or even individual "red team exercises" to ensure there is sufficient independent analysis. Rather, such independent analysis must become a habitual analytic practice for *all* analysts. The decentralization of the Intelligence Community's analytic bodies will naturally contribute to independent and divergent analysis, and we believe that the Mission Managers we propose will play a valuable role in identifying and encouraging independent analysis in their topic areas. But the Intelligence Community must also ensure that analysts across the Community are trained to question their assumptions and make their arguments explicit. Alternative analysis should be taught in the very first analyst training courses as a core element of good analytic tradecraft. It is to this topic—the training of analysts—that we next turn.

IMPROVING TRADECRAFT THROUGH TRAINING

A common theme from our case studies is that the fundamental logical and analytic principles that should be utilized in building intelligence assessments are often inadequately applied. There are several reasons for this. Key among these is a leadership failure; managers of analysts have neglected to demand the highest standards of analytic craft. This management weakness has been compounded in recent years by the lack of experience among analysts, caused

by the more than 33 percent decline in the number of analysts from the latter part of the 1980s through most of the 1990s. On top of the numerical reduction, many of the *best* analysts left during this period because they were the ones who could easily get jobs outside of government. The outflow of knowledge was even greater than the outflow of people.

The Intelligence Community started slowly to hire more analysts in the late 1990s, and recent congressional and executive branch actions are now resulting in further expansion of the analytic corps. As a result, the Intelligence Community is now populated with many junior analysts and few mentors. And the focus on current intelligence has meant that few analysts are given the time to develop expertise, while managers have little time to develop management and mentoring skills.

These difficulties have reduced the quality of finished intelligence. When we reviewed finished intelligence, we found egregious examples of poor tradecraft, such as using a piece of evidence to support an argument when the same piece also supported exactly the opposite argument—and failing to note this fact. In some cases, analysts also failed to update or correct previously published pieces, which led other analysts and policymakers to make judgments on faulty or incomplete premises.

But far and away the most damaging tradecraft weakness we observed was the failure of analysts to conclude—when appropriate—that there was not enough information available to make a defensible judgment.[14] As much as they hate to do it, analysts must be comfortable facing up to uncertainty and being explicit about it in their assessments. Thankfully, we have found several instances of recent efforts by individual analysts to clearly admit what they do and do not know. In particular, a recent National Intelligence Estimate used new processes to ensure that source information was carefully checked for accuracy before inclusion in the estimate. In addition, the Estimate clearly highlighted the intelligence collection gaps on the topic and analysts' level of confidence in their judgments. In our classified report we discuss the particulars of this Estimate in greater depth. Still, these efforts have not been institutionalized, nor are they widespread. We heard many times from users of intelligence that they would like analysts to tell them up front what they don't know—something that intelligence analysts apparently do too infrequently.

Recommendation 8

The Intelligence Community must develop a Community program for training analysts, and both analysts and managers must prioritize this career-long training.

The Intelligence Community must reverse the erosion of analytic expertise that has occurred over the last 15 years. Analytic reasoning must be more rigorous and be explained in clearer terms in order to improve both the quality and credibility of intelligence. Specifically, analysts should take pains to write clearly, articulate assumptions, consistently use caveats, and apply standard approaches to sourcing. A renewed focus on traditional tradecraft methods needs to be augmented with innovative methodologies and tools that assist the analyst without inhibiting creativity, intuition, and curiosity.

This strengthening of the analytic workforce can only occur through a dedicated effort by the Intelligence Community to train analysts throughout their careers. A structured Community program must be developed to teach rigorous tradecraft and to inculcate common standards for analysis so that, for instance, it means the same thing when two agencies say they assess something "with a high degree of certainty." Equally important, managers and analysts must be held accountable for ensuring that analysts continue to develop expertise throughout their careers. The excuse, "I didn't have time for training," is simply unacceptable. This responsibility of both managers and analysts for continued tradecraft training should be made part of all performance evaluations.

Another critical element of training for analysts, and one that has been long lacking in the Intelligence Community, concerns their understanding of intelligence *collection*. Today, analysts receive too little training on collection capabilities and processes, and the training they do receive does not adequately use practical exercises to help analysts learn how to build effective collection strategies to solve intelligence problems. This fundamental ignorance of collection processes and principles can lead to serious misjudgments, and we recommend that the Intelligence Community strengthen analyst training in this area. In our classified report we point to areas in other intelligence agencies' training programs that we believe could be improved, but that cannot be discussed in an unclassified report.

What Denial and Deception (D&D) Means for Analysis

State and non-state actors either with or seeking to develop WMD materials and technologies all practice robust denial and deception techniques against U.S. technical collection. We must significantly reduce our vulnerability to intelligence surprises, mistakes, and omissions caused by the effects of denial and deception (D&D) on collection and analysis. To do so, the Community must foster:

- ***Greater awareness of D&D among analysts,*** including a deeper understanding of what other countries know about our intelligence capabilities, as well as the D&D intentions, capabilities, and programs of those countries.
- ***Greater specification by analysts of what they don't know and clearer statements of their degree of certainty.*** Analysts should also work more closely with collectors to fully exploit untapped collection opportunities against D&D targets, and to identify and isolate any deceptive information.
- ***Greater appreciation for the capabilities and limitations of U.S. collection systems.***
- ***Greater use of analytical techniques that identify the impact of denial and the potential for deception.*** Analysts must understand and evaluate the effects of false, misleading, or even true information that intelligence targets may have injected into the collection stream to deceive the United States.

Recommendation 9

The Intelligence Community must develop a Community program for training managers, both when they first assume managerial positions and throughout their careers.

Managerial training must also be vastly expanded throughout the Intelligence Community. Although scattered training is available, the Intelligence Community currently has no systematic, serious, or sustained management training program, and none that readily allows for cross-agency training—even though management problems can be similar across agencies. CIA managers,

for example, receive a small portion of the training provided to their military counterparts.[15] And we are dismayed that some in the Intelligence Community resisted programs such as merit-based pay due to a mistrust of managers' ability to accurately and fairly measure performance.

Prospective managers should be given extensive management training before assuming their responsibilities, and current managers should be enrolled in refresher training courses on a regular basis. A well-trained management and leadership corps within the Intelligence Community is vital to the health of analysis (and collection), and the Community is currently suffering the consequences of its absence. To the degree that a few individuals at the CIA have already recognized this problem, and are designing programs to address it, we commend them.

Although we hesitate to prescribe any specific level of centralization for analytic and managerial training, we do suggest that some of the training be Community-wide, perhaps housed in our proposed National Intelligence University or done through an online education program.[16] We do so in full recognition that individual agencies may want to conduct their own training because their workforce requires specialized skills, and that some resist centralized training on the grounds that training should engender a strong affiliation among analysts for their particular agency.

Notwithstanding these objections, as discussed in our chapter on Management, we believe that the creation of the DNI provides a unique opportunity to reconsider implementing some elements of Community training. The benefits will be enormous: it will teach common tradecraft standards, standardize teaching and evaluation, foster a sense of Community among analysts, and, we hope, provide analysts with a wider range of training opportunities throughout their careers. It may also create economies of scale in training costs. For these reasons, we strongly encourage joint training whenever feasible.

MAKING ANALYSIS MORE TRANSPARENT

Training analysts and managers to use better "tradecraft" is only half the battle; rigorous analytic methods must be demanded in every intelligence product. One way of doing so—and at the same time ensuring that customers are confident in the intelligence they receive—is to make the analytic process

more transparent. Although we recognize that real security issues make total transparency impossible, we fear that protecting sources and methods has resulted in the shrouding of analysis itself, not just the intelligence on which it is based. This tendency must, we believe, be actively resisted.

Recommendation 10

Finished intelligence should include careful sourcing for all analytic assessments and conclusions, and these materials should—whenever possible in light of legitimate security concerns—be made easily available to intelligence customers.

We recommend forcing analysts to make their assumptions and reasoning more transparent by requiring that analysis be well sourced, and that all finished intelligence products, either in paper or in digital format, provide citations to enable user verification of particular statements. This requirement is no more rigorous than that which is required in law, science, and the social sciences, and we see little reason why such standards should not be demanded of the Intelligence Community's analysts. Analysts are generally already expected to provide sources for internal review; including this information in finished analysis would simply increase the transparency of the process.

We further recommend that customers have access to the raw intelligence reporting that supports analytic pieces whenever possible, subject to legitimate security considerations. For many intelligence customers, especially senior policymakers and operators, a general description, such as State Department "diplomatic reporting" simply does not provide the confidence needed to take quick and decisive action.[17] Where a user accesses finished intelligence electronically, he should be able to link directly to at least some portion of the raw intelligence—or to underlying finished intelligence—to which a judgment is sourced.

Requiring that citations be routinely available and linked to source documents need not preclude analysts from making judgments or inferences; rather, the availability of such materials will simply enable users to distinguish quickly between those statements that are paraphrased summaries of intelligence reporting, and those that are analytic judgments that draw inferences from this reporting. Of course, some analysts might worry that such a system would

essentially sideline the analyst, making his or her work irrelevant because all of his or her hard calls could be "questioned" by returning to the original sources and performing the analysis independently. We do not, however, think this is inherently bad. Intelligence customers should be able to question judgments, and analysts should be able to defend their reasoning. In the end, such a reform should bolster the stature of good analysts, as policymakers and operators come to see their analytic judgments as increasingly accurate and actionable.

Recommendation 11

The analytic community should create and store sourced copies of all analytic pieces to allow readers to locate and review the intelligence upon which analysis is based, and to allow for easy identification of analysis that is based on intelligence reports that are later modified.

We recommend that the DNI create a system to electronically store sourced versions of analytic pieces and ensure that source information is easily accessible to intelligence users, consistent with adequate security permissions. Of course, to make such electronic storage and accessibility possible one needs first to have a truly integrated information sharing environment and shared information technology systems—a considerable challenge given the inadequacies of today's information technology environment, on which we comment more fully in Chapter Nine (Information Sharing).

The DNI should also encourage the development of a system that enables Intelligence Community personnel to update intelligence information that has been judged to be unreliable, of increased or decreased certainty, or simply retracted. These updates must be electronically flagged in the intelligence reports themselves as well as any analytic products citing to the reports. Such tracking systems have existed in other fields for decades (*e.g.*, Lexis and Westlaw for the legal world).[18]

Above and beyond the technical constraints to implementing such a system, there are several barriers that have blocked these reforms in the past. For example, CIA's Directorate of Operations maintains a close hold on its highly sensitive reporting, often with good reason. Making this raw reporting accessible to policymakers and intelligence officers across the Commu-

nity raises several security and counterintelligence-related concerns. Furthermore, it is questionable to what degree *all* policymakers will need access to raw reporting.

But none of these issues explains why the Intelligence Community's efforts in this vein are still in such a stage of infancy. While there will be information that cannot be provided to intelligence customers, many decisionmakers can and do read intelligence reporting at the same time as the analysts who receive it. Further, access to an analytic product is typically limited to those who are cleared to read the intelligence reports on which it is based. The easy availability of source information, related reporting, and other finished intelligence products, along with a system to clearly identify old intelligence that has been reconsidered in one way or another, will benefit both analysts and customers. Analysts will, we believe, do their work more meticulously and accurately, while customers will be able to better understand the products they receive and know whether the Community continues to stand behind the intelligence.

IMPROVING SCIENTIFIC, TECHNICAL, AND WEAPONS INTELLIGENCE

Recommendation 12

The DNI should develop and implement strategies for improving the Intelligence Community's science and technology and weapons analysis capabilities.

A specific subset of analysts within the Intelligence Community is responsible for assessing emerging threats to U.S. interests resulting from advances in foreign science and technology (S&T) and weapons developments. Using specialized scientific and technical expertise, skills, and analytic methodologies, these analysts work on some of today's most important intelligence issues, including counterproliferation, homeland security, support to military operations, infrastructure protection, and arms control. We are therefore concerned that a recent Intelligence Science Board study concluded that the Intelligence Community's current S&T intelligence capability is "not what it could be and not what the nation needs."[19]

The Intelligence Science Board study and our own research found that the Intelligence Community's ability to conduct S&T and weapons analysis has

not kept pace with the changing security environment.[20] The board's study noted the Intelligence Community was particularly vulnerable to surprise by "rapidly changing and readily available emerging technologies whose use by state and non-state actors, in yet unanticipated ways, may result in serious and unexpected threats."[21] The S&T areas of most concern include biological attacks, nuclear threats, cyber warfare, Chinese technology leapfrogging, and the impact of commercial technologies on foreign threats.[22] In addition, current analysis often fails to place foreign S&T and weapons developments in the context of an adversary's plans, strategy, policies, and overall capabilities that would provide customers with a better understanding of the implications for U.S. security and policy interests.[23] One senior Administration official interviewed by the Commission staff described the Intelligence Community's capability to conduct this kind of all-source S&T and weapons analysis as "pretty poor" and "mediocre at best."[24]

The state of the Intelligence Community's S&T and weapons analysis capabilities should be a key issue for the DNI, given the importance of these fields in providing warning and assessments of many of today's critical threats. In addition to hiring more analysts with technical and scientific skills and experience, the Intelligence Community would benefit from more contact with outside technical experts who could conduct peer reviews and provide alternative perspectives. In addition, resources should be set aside for conducting in-depth and multidisciplinary research and analysis of emerging technologies and weapon developments to help the Community keep pace with the ever-changing security environment. The use of analytical methodologies, such as red teaming, scenario analyses, and crisis simulations, to explore and understand the impact of new technologies and weapons on U.S. interests should also be encouraged to help analysts guard against technology surprise.

To ensure progress will be made in the future, we recommend that the DNI designate a Community leader for developing and implementing strategies for improving the Intelligence Community's S&T and weapons analysis capabilities. This person should report to the DNI on a periodic basis on the status of the Community's relevant capabilities and make recommendations on where further improvements are needed.

SERVING INTELLIGENCE CUSTOMERS

Analysts are the link between customers and the Intelligence Community. They provide a conduit for providing intelligence to customers and for conveying the needs and interests of customers to collectors. This role requires analysts to perform a number of functions. Analysts must assess the available information and place it in context. They must clearly and concisely communicate the information they have, the information they need, the conclusions they draw from the data, and their doubts about the credibility of the information or the validity of their conclusions. They must understand the questions policymakers ask, those they are likely to ask, and those they should ask; the information needed to answer those questions; and the best mechanisms for finding that information. And as analysts are gaining unprecedented and critically important access to operations traffic, they must also become security gatekeepers, revealing enough about the sources for policymakers to evaluate their reporting and conclusions, but not enough to disclose tightly-held, source-identifying details.

Analysts fulfill these functions through interactions with a wide range of intelligence customers, who run the gamut in terms of rank, area of responsibility, and understanding of intelligence. "Typical" customers include not only the President and senior policymakers, but also members of Congress, military commanders, desk officers in executive agencies, law enforcement officers, customs and border patrol officials, and military units in the field. We do not attempt to examine each of these relationships, but we do note some challenges in this area. Specifically, we address how the Intelligence Community might modernize some customer relationships, some components of an "appropriate" relationship between analysts and customers, and how the President—and to a lesser degree other senior policymakers—should be supported.

Modernizing the Analyst-Customer Relationship

Recommendation 13

The DNI should explore ways to make finished intelligence available to customers in a way that enables them—*to the extent they desire*—to more easily find pieces of interest, link to related materials, and communicate with analysts.

The Intelligence Community must distribute its products more efficiently and effectively. Today's policymaker receives intelligence in almost the same way as his 1985 predecessor; most intelligence products from the CIA's Directorate of Intelligence, for example, are still delivered in hardcopy. For some customers, this may remain the preferred method of receiving intelligence. For others with different needs or preferences—and we have heard from some of them—the Intelligence Community should consider ways to modernize intelligence distribution.

Some modernization has occurred; most notably, a limited number of Washington policymakers can access some intelligence products through the Defense Department's secure networks—JWICS and Intelink—at their desk. But the "populating" of these networks varies across agencies and by product type. For example, INR and DIA routinely place their publications on these secure networks, and a large percentage of finished intelligence products related to counterterrorism can be found online. By contrast, CIA sharply limits the use of its finished intelligence on these networks, citing the need to protect its human sources. And even when intelligence is available on electronic networks, the interfaces are clumsy and counterintuitive—far below the presentation of online publishers such as the *Washington Post*.

This state of affairs is markedly inferior to the state of the practice in private industry. Most customers of intelligence products cannot search electronic libraries of information or catalogues of existing products. They cannot query analysts in real time about needed information or upcoming products. They cannot link finished intelligence documents together electronically to create a reference trail. They cannot easily review research programs to provide suggestions or recommendations. They cannot explore thoughts and views with analysts in an informal online environment. They cannot read informal mes-

sages alerting them to new information which may include analysts' preliminary thoughts or judgments on an item. They cannot tailor information displays to their needs. They cannot reshape raw data into graphics and charts. They cannot access different intelligence media electronically.

This is not an area in which there is only one right answer; there are many ways to provide up-to-the-minute, in-depth information to policymakers in user-friendly formats. We also recognize that because of the dramatic effects an electronic system would have on the way the Intelligence Community does its work and because of substantial security concerns, any new program along these lines will require a great deal of additional thought and planning. Nevertheless, we believe that even in the relatively near future the benefits of an integrated electronic system will outweigh the risks, and it will become more necessary as a new generation of customers—with a preference for the flexibility of digital technology—reaches higher levels of government.

Components of the Analyst-Customer Relationship

Regardless of how customers receive intelligence, both analysts and customers have to recognize that certain exchanges between the two are appropriate and should be encouraged. Perhaps most importantly, we believe it is critical that customers engage analysts. It is the job of the analyst to express clearly what the analyst knows, what the analyst doesn't know, what the analyst thinks, and why—but if the analyst does not, the customer must insist that the analyst do so. If necessary, the customer should challenge the analyst's assumptions and reasoning. Because they are "keepers of the facts," analysts can play a decisive role in policy debates, a role that has temptations for analysts with strong policy views of their own. A searching examination of the underlying evidence for the analysts' factual assertions is the best way to reassure policymakers that the analysts' assertions are well-grounded. We reject any contention that such engagement is in itself inappropriate or that the risk of "politicizing" intelligence cannot be overcome by clear statements to analysts as to the purpose of the dialogue. When an analyst leaves a policymaker's office feeling thoroughly cross-examined and challenged to support his premises, that is not politicization; it is the system working at its best. Only through active engagement of this sort will intelligence become as useful as it can be.

Analysts also have a responsibility to tell customers about important disagreements within the Intelligence Community. We were told by some senior policymakers that it sometimes took weeks to get an answer to a question—not because the answer was difficult to obtain, but because analysts were hesitant to admit to Intelligence Community disagreement on an issue. This is not how intelligence should function. Analysts must readily bring disagreement within the Community to policymakers' attention, and must be ready to explain the basis for the disagreement. Such disagreement is often a sign of robust independent analysis and should be encouraged.

In addition to conveying disagreements, analysts must also find ways to explain to policymakers degrees of certainty in their work. Some publications we have reviewed use numerical estimates of certainty, while others rely on phrases such as "probably" or "almost certainly." We strongly urge that such assessments of certainty be used routinely and consistently throughout the Community. Whatever device is used to signal the degree of certainty—mathematical percentages, graphic representations, or key phrases—all analysts in the Community should have a common understanding of what the indicators mean and how to use them.

Finally, analysts and Intelligence Community leaders have a responsibility to take note, whenever possible, of what their customers are doing and saying, and to tell those customers when actions or statements are inconsistent with existing intelligence. We do not mean to suggest that analysts should spend all of their waking hours monitoring policymakers, or that analysts should have a "veto" over policymaker statements. Rather, when aware of upcoming speeches or decisions, analysts should make clear that they are available to vet intelligence-related matters, and analysts should—when necessary—tell policymakers how their statements diverge from existing intelligence. Having fulfilled this duty, analysts must then let politically-accountable policymakers determine whether or not a statement is appropriate in light of intelligence judgments.

Serving the President and Senior Policymakers

The new legislation designates the DNI as the person primarily responsible for ensuring that the President's day-to-day intelligence needs are met.[25] This means that the Office of the DNI, not the Director of the Central Intelligence Agency, should have the final authority over the content and production of the

President's Daily Brief (PDB)—or whatever other form intelligence support to the President may take.

We also believe that the DNI will have to work closely with the President and the National Security Council to reconsider how intelligence should best be presented to the President, because we are dubious that the PDB—in its current incarnation—is the right answer.

Our case studies, primarily Iraq, highlight several flaws indicating a need to rethink the PDB.[26] PDB pieces are typically limited by space constraints. While sophisticated, in-depth analysis can be presented in this abbreviated fashion, the task is considerably more difficult than drafting a more immediate, less research-intensive piece that updates the reader on current events and provides a more limited, near-term analytic focus. As a result, we worry that individual PDB articles fail to provide sufficient context for the reader. This view was reinforced by one senior intelligence officer's observation that policymakers are sometimes surprised to find that longer, in-depth intelligence reporting provides a different view from that conveyed by the PDB. The same individual noted that when a policymaker is given a piece of information about a certain subject, the policymaker will often ask questions about the information, leading to follow-up on that subject, thereby exacerbating the current intelligence bias.[27] Moreover, the PDB staff tends to focus on today's hot national security issues, or on issues that attracted the President's interest the last time they came up. This can lead to repeated reporting on a given topic or event; a drumbeat of incremental "hot news" articles affects a reader much differently than the same information presented in a longer, contextualized piece that explains the relationship between the various reports. Finally, the PDB sometimes includes excessively "snappy" headlines, which tend to misrepresent an article's more nuanced conclusions, and which are, in our view, unnecessary; a two or three-word indicator of the piece's subject (such as "North Korea-Nuclear") would tell policymakers which pieces were of most interest to them without obscuring the subtle contours of an issue raised in the text.

Having identified these potential problems, we are hesitant to suggest how the PDB process should be altered. Only the President can say for certain how often and in what format he prefers to receive national intelligence information. We do, however, recognize that the creation of the DNI will shift what

has been a CIA-centric PDB process to more of a Community one—shepherded by the Office of the DNI.

Recommendation 14

The President's Daily Brief should be restructured. The DNI should oversee the process and ensure a fair representation of divergent views. Reporting on terrorism intelligence should be combined and coordinated by the DNI to eliminate redundancies and material that does not merit Presidential action.

Regardless of the structure of the PDB process, the DNI will need to respond to the demands of senior advisors and the President. We recommend that the DNI create an analytic staff too small to routinely undertake drafting itself, but large enough that its members would have expertise on a wide range of subjects. The staffers would task the appropriate experts and agencies to draft responses to decisionmaker requests. They could also perform last minute editing and would—in every case—ensure that the pieces reflect any differences of opinion in the Community.[28] In our view, it is simply not enough to present dissenting views from the Intelligence Community only in longer, more formal assessments like National Intelligence Estimates. Rather, because policymakers tend to be significantly influenced by daily intelligence products, we believe it is essential that those products offer as complete a perspective on an issue as is feasible. This is not to suggest that the production of each daily briefing for the President or others should recreate a mini-NIE process; in many cases, relatively few intelligence agencies need be involved. But when agencies have sharp differences, the DNI's analytic staff should be responsible for ensuring that the final memorandum clearly reflects these competing conclusions and the reasons for disagreement.

Equally important, we believe that the DNI should seek to combine—with the President's concurrence, of course—the three primary sources of intelligence that now reach the President. Currently, in addition to the PDB, the President receives the President's Terrorism Threat Report (PTTR), which is prepared by the National Counterterrorism Center and is appended to each day's PDB. The President may also be verbally briefed by the Director of the FBI who uses material from a "Director's Daily Report" prepared by his staff.

We have reviewed these materials and discussed the briefings with many regular participants. There are plainly redundancies that should be eliminated, but we are also concerned that the channels conveying terrorism intelligence are clogged with trivia. One reason for this unnecessary detail is that passing information "up the chain" provides bureaucratic cover against later accusations that the data was not taken seriously. As one official complained, this behavior is caused by bureaucracies that are "preparing for the next 9/11 Commission instead of preparing for the next 9/11." It may be difficult to stem this tide, but the new DNI is in the best position to bring order to the process. We recommend that the DNI be given clear responsibility for combining terrorism intelligence into a single, regular Presidential briefing (whether a daily briefing is required should depend on the pace of events). This briefing would resemble and would perhaps be combined into the PDB.

In the same vein, several senior officials told us that they read the PDB not so much for its content (for it often did not necessarily include especially critical information) as much as to stay apprised of matters on which the President is briefed. In this light, although the DNI and the PDB staff must be free to make a professional judgment about the intelligence to present on any given day, we recommend that the DNI encourage suggestions from policymaking agencies like State and Defense about topics that could usefully be presented in the President's briefing. By taking this step the PDB would likely become more attuned to a wider variety of pressing national security issues.

We fully recognize that the DNI's role calls for a delicate balance. It will be tempting for the DNI's analysts to become the primary drafters themselves, and analysts in individual agencies will continue to face demands from those in their chain of command to respond to requests directly. The former would turn the office of the DNI into one more analytic entity putting forward its own views. The latter problem recreates the situation we have today, which often results in a multiplicity of uncoordinated views appearing before senior decisionmakers. The DNI's analytic cadre, whose responsibility it is to understand and to put forward the views of the Community's experts, wherever located, must ensure that analytic differences in the Community are not suppressed and, equally important, are not presented to decisionmakers in a piecemeal fashion that forces senior officials to sort out the differences themselves.

RETAINING THE BEST ANALYSTS

The Intelligence Community is unlikely to have the funding necessary to rely exclusively—or even primarily—on economic incentives to recruit and retain the best and the brightest. The Community, however, has always offered analysts something more: the opportunity to play a role in shaping the decisions of the nation's top leaders and to help maintain the security of our nation. To the extent that the Community loses sight of this as a motivating factor for its employees, it loses its most valuable tool for recruitment and retention.

Recommendation 15

The Intelligence Community should expand the use of non-monetary incentives that remind analysts of the importance of their work and the value of their contributions to national security.

Recognize good performers. The Intelligence Community should look for ways to ensure that the best analysts are recognized both within the Community and by decisionmakers outside of the Community. The fact that the Community on the whole works in relative anonymity makes this recognition all the more necessary. Analysts who are viewed as experts get the opportunity to do exactly what analysts are hired to do—play a part in shaping U.S. policy. In turn, analysts who have the chance to sit face-to-face with top-level decisionmakers are motivated in a very personal way to do their best.

Provide travel, training, rotations, and sabbaticals. All analysts are not alike, and not all opportunities for professional development will appeal to all equally. But giving analysts time to do the things they most want to do, particularly when the activities also contribute to the development of their expertise, is beneficial to everyone. One DIA manager told us that fully funding a robust travel budget would be far cheaper than paying salaries on a par with those paid by contractors, and would help a great deal in keeping analysts motivated and interested.[29] Other analysts are likely to find other activities more appealing, from full-time academic training, to policy rotations, to stints in the Office of the DNI or other agencies within the Community.

Permit careers to focus on the analysts' areas of interest. Analysts also differ in their preferred approaches to their careers. Some enjoy being generalists,

moving among all types of accounts and bringing a fresh perspective; others have a strong interest in a certain type of analysis—such as conventional weapons—or an area of the world, and might choose to spend time on a variety of similar accounts. Still others seek to specialize on fairly focused subject matters. The Intelligence Community benefits from all of these career paths, and in the best of all worlds, analysts would be able to follow the one best suited to their interests. The nature of the intelligence business will never allow for such a perfect fit; some specialists will need to remain on an account after their interest in it has waned, and some analysts will be pulled from where they are happiest to respond to an emerging crisis. But the goal should be to get it right for as many analysts as possible. Doing so is an enormously powerful retention tool. Managers of technical analysts explained to us that they had a great deal of difficulty retaining analysts because they came in expecting to work on areas in which they had developed expertise, but were pulled by the demands of the job into other areas that they found less interesting.[30] We expect that the Mission Managers will be able to place more focused attention on long-range planning and generate an increased understanding of where knowledge and expertise reside—and thus better position the Community to respond to emerging crises in a thoughtful way and reduce the numbers of analysts forced into jobs they dislike.

Provide tools and support. Managers also complained that analysts often find that the tools and technology available in the Intelligence Community fall short of what they use in school, at home, or in the private sector.[31] Moreover, analysts across the board face declining administrative support. Among other things, analysts typically must do desktop publishing, maintain files of classified materials not available electronically, manage contracts, and perform logistical tasks associated with travel or training. In other words, analysts often view their counterparts in the private sector as having better tools and better support that enable them to spend their time and energy on core tasks. Giving analysts what they need to do their job and ensuring that they spend their time as *analysts*, not clerks or administrative aides, would emphasize that their time and skills are valued.

LEARNING FROM PAST MISTAKES

The new intelligence reform legislation requires the DNI to assign an individual or entity the responsibility to ensure that finished intelligence products are timely, objective, independent of political considerations, based on all sources

of available intelligence, and grounded in proper analytic tradecraft. In the course of conducting relevant reviews, this entity is further directed to produce a report of lessons learned.[32]

Recommendation 16

Examinations of finished intelligence should be routine and ongoing, and the lessons learned from the "post mortems" should be incorporated into the intelligence education and training program.

Iraq, Libya, and Afghanistan have offered opportunities for the Intelligence Community to compare its assessments with the ground truth and examine the sources of the disparities. We have already seen evidence that the lessons learned from Iraq are being incorporated by analysts covering other countries or intelligence topics. Analysts are increasingly careful to explain their analytical baseline in their products, and attribute the sources of intelligence underlying it. The Intelligence Community, analysts say, has adopted the "rule of elementary school math class," in that its analysts are dedicated to "showing our work" to prevent the "layering of analysis."[33]

This is an area in which the Intelligence Community should learn from the Department of Defense, which has an especially strong, institutionalized process for benefiting from lessons learned. In our classified report, we discuss a Defense Department "lessons-learned" study that we found particularly impressive, but that we cannot elaborate upon here. Intelligence Community lessons-learned efforts (such as CIA's Product Evaluation Staff) had less success, in part because they do not have sufficient resources or possess much prestige within intelligence agencies. Nor do we think that, in general, intelligence agencies should be responsible for "grading their own papers." The intelligence reform legislation recognizes the need for a separate body that conducts reviews of analysis, a welcome idea that should be fully embraced by the Community.

CONCLUSION

The changes that we recommend are significant departures from the current way in which the Community conducts the business of analysis. Some run counter to long-standing, embedded practices, and we are mindful that they

may be resisted by analysts and managers alike. We believe, however, that these changes are essential to improving the Community's capability to accurately assess threats and to provide timely, relevant, thoughtful support to policymakers. Intelligence analysis faces unprecedented challenges; unprecedented measures to strengthen the analytical process are well warranted.

ENDNOTES

[1] U.S. Senate, *The Final Report of the Select Committee To Study Governmental Operations with Respect to Intelligence Activities* (April 26, 1976) (*i.e.*, Church Committee Report); Permanent Select Committee on Intelligence, U.S. House of Representatives, *IC21: Intelligence Community in the 21st Century* (1996); Commission to Assess the Ballistic Missile Threat to the United States (*i.e.*, Rumsfeld Commission), *Side Letter to the President* (March 18, 1999); CIA, *The Jeremiah Report: The Intelligence Community's Performance on the Indian Nuclear Tests* (June 1, 1998); Markle Foundation Task Force, *Creating a Trusted Information Network for Homeland Security* (Dec. 2003); National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (*i.e.*, The 9/11 Commission Report) (2004); Council on Foreign Relations, *Making Intelligence Smarter: The Future of U.S. Intelligence: Report of an Independent Task Force* (1996); Commission on the Roles and Capabilities of the United States Intelligence Community (*i.e.*, Aspin-Brown Commission), *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (1996); *Report of the Commission on Organization of the Executive Branch of the Government* (*i.e.* Hoover Commission Report) (1949).

[2] Staff review of House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence Markups of Intelligence Authorization Bills, 1991-2005.

[3] Interview with senior intelligence official (Sept. 22, 2004).

[4] The CIA has had similar programs in the past whereby the agency introduced analysts who were tools experts to work alongside other analysts. These analysts were just like their analytic colleagues, except that they were also specialists in how to use analytic technologies and could help counterparts learn to use these tools to structure research problems. CIA Office of Research and Development, *Office of East Asian Analysis Testbed Project Final Report* (Sept. 30, 1994).

[5] Interview with biosecurity expert (Feb. 4, 2005).

[6] Inter-agency Information Sharing Working Group, *Consolidated Report* (Dec. 14, 2004) at p. 5. We provided an additional footnote illustrating the magnitude of this challenge in our classified report.

[7] CIA Office of Research and Development, *Office of East Asian Analysis Testbed Project Final Report* (Sept. 30, 1994).

[8] Interview with senior In-Q-Tel official (Feb. 3, 2005). In addition, a senior manager of analysis told us he knew there is a need to make better use of open sources but that this could not be achieved without assistance in the form of preliminary correlation of the data. Interview with senior CIA DI official (Feb. 10, 2005).

[9] Interview with senior In-Q-Tel official (Feb. 3, 2005).

[10] Interview with CIA analysts (Jan. 24, 2005).

[11] Interview with former CIA WINPAC analysts (Nov. 10, 2004).

[12] These formal alternative analysis programs are also reinforced by the existence of multiple analytic units in the Community, which often reach different analytic conclusions.

[13] The DNI is statutorily required to assign responsibility "for ensuring responsibility that, as appropriate, elements of the Intelligence Community conduct alternative analysis." Intelli-

gence Reform and Terrorism Prevention Act of 2004 at § 1017, Pub. L. No. 108-458 (hereinafter "IRTPA").

[14] Chapter Three (Afghanistan).

[15] Interview with senior CIA official.

[16] There currently exist several very successful joint training programs. The Joint Military Intelligence College, for example, currently operates a very successful program—a structured intermediate/advanced curriculum for Intelligence Community officers across the Community. At the same time, many similar efforts have failed for various reasons, including insufficient funding and lack of bureaucratic clout. The Defense Department Chancellor for Civilian Education's program is one such example of an unsuccessful cross-agency effort. Interview with former senior staff of the defunct Department of Defense Office of the Chancellor for Civilian Education and Development (Jan. 13, 2005).

[17] Some, but not most, of the finished intelligence provided to the Commission included lists of reference numbers identifying particular sources, but we understand that such lists are not routinely provided to policymakers. In any case, these lists provide no indication of how one could determine which specific document supported facts included in the piece.

[18] We recognize that the DCI is currently working to establish Community procedures for such a system, and we commend this development. Chapter One (Iraq) provides a detailed discussion of how analysts and intelligence users continued to use reporting considered unreliable.

[19] DCI Intelligence Science Board Task Force, *The State of Science and Technology Analysis in the Intelligence Community* (April 2004) at p. xiii (hereinafter "ISB Report").

[20] *Id.* at p. xiii; Interview with senior intelligence official (Oct. 7, 2004); Interview with senior DIA analyst (Sept. 23, 2004).

[21] ISB Report at pp. 26-27.

[22] *Id.* at p. 27.

[23] *Id.* at pp. 26, 28; Interview with administration official (Sept. 30, 2004); Interview with administration official (Sept. 10, 2004).

[24] Interview with senior administration official (Oct. 12, 2004).

[25] IRTPA at § 1011.

[26] In addition, several senior policymakers expressed concerns about the utility of the PDB in its current incarnation.

[27] Interview with senior intelligence analyst (Nov. 8, 2004).

[28] We understand that the CIA is already moving in this direction and we commend it for doing so.

[29] Interview with DIA analysts and managers (Oct. 26, 2004).

[30] *See, e.g.*, Interview with CIA WINPAC analysts (Oct. 14, 2004).

[31] *Id.*

[32] IRTPA at § 1019.

[33] Interview with DIA analysts (Nov. 22, 2004).