Casting aside the perceived—and I must admit the occasionally real—excitement of secret operations, the absolute essence of the intelligence profession rests in the production of current intelligence reports, memoranda and National Estimates on which sound policy decisions can be made.

—Richard Helms, *A Look Over My Shoulder*

As Director of Central Intelligence (DCI) Richard Helms (1966–1973) observed, despite all the attention lavished on the operational side of intelligence (collection and covert action), analysis is the mainstay of the process. Intelligence analysis provides civil and military policy makers with information directly related to the issues they face and the decisions they have to make. Intelligence products do not arrive on policy makers’ desks once or twice a day, but in a steady stream throughout the day. Certain products, particularly the daily intelligence reports and briefings, are received first thing in the morning, but other intelligence reports can be delivered when they are ready or may be held for delivery at a specific time.

Although not all intelligence practitioners agree, the ongoing production and delivery of intelligence can have a numbing effect on policy makers. Intelligence analysis can become part of the daily flood of information—intelligence products; commercially provided news; reports from policy
offices, embassies, and military commands; e-mails; and so on. One of the challenges for intelligence is to make itself stand out from this steady stream of information.

Intelligence can be made to stand out in two ways. One is to emphasize the unique nature of the intelligence sources. But this option is not the preferred choice of intelligence officials, who believe that they are much more than just conduits for their sources. The other way for intelligence to achieve prominence is to produce analysis that stands out on its own merits by adding value. The value added includes the timeliness of intelligence products, the ability of the community to tailor products to specific policy makers’ needs, and the objectivity of the analysis. One analyst who had been a presidential brief put it this way: “My value was telling the president something he didn’t already know about something he needed to know.” But the fact that value-added intelligence is discussed as often as it is within the intelligence community suggests that it is not achieved as often as desired.

Major Themes

Prescribing how to produce value-added intelligence—or how to measure the frequency with which it is produced—is difficult because intelligence officers and their policy clients do not agree on what adds value. For policy clients, value added is an idiosyncratic and personal attribute.

Analysis is much more than sitting down with the collected material, sifting and sorting it, and coming up with a brilliant piece of prose that makes sense of it all. Major decisions have to be made in the analytical process, and several areas of controversy have proved to be resilient or recurrent.

**Formal Requirements.** In the ideal intelligence-process model, policy makers give some thought to their main requirements for intelligence and then communicate them to the intelligence managers. Such a formal process has not appeared often in the history of the intelligence community, leaving managers to make educated guesses about what intelligence is required.

Some people argue that a less formal process is, in reality, much better than the presumed ideal one, because most of the requirements of intelligence are fairly well known and do not need to be defined. For example, most people, if asked to name the main U.S. intelligence priorities during the cold war, would mention a number of Soviet-related issues. Even in the less clear post–cold war period before the September 2001 terrorist attacks, a similar exercise would yield such answers as narcotics, terrorism, proliferation, Russia’s reform and stability, and the regional trouble spots of the moment,
such as Iran, the Middle East, and North Korea. The list parallels the U.S. intelligence priorities as stated in the Bill Clinton administration’s Presidential Decision Directive 35. After September 2001, terrorism became the primary, but not the sole, focus of intelligence.

The real importance of the requirements process may lie in giving the intelligence community some sense of priority among the requirements. Formal discussions about priorities between senior policy makers and intelligence officers tend to revolve around relative degrees of importance instead of issues that have been added to the priorities list or overlooked. Assigning priorities is especially important and difficult in the absence of a single overwhelming issue, as was the case from roughly 1991 (the end of the Soviet Union) until 2001. When several issues are considered to be of roughly equal importance, no single one of them has priority. However, this seeming lack of focus may reflect the reality of national security interests. In such a circumstance the intelligence managers must then make critical decisions about the allocation of collection and analytical resources among several equally important and competing issues.

Some people also misunderstand the goal of the priority process and view it as a forecast of the issues that will be important in the near future. A priorities process is an expression of areas of interest and their relative importance to one another, not a forecast of which of these issues will be most prominent. Indeed, most people who manage priorities systems recognize that there will inevitably be issues that arise that were not foreseen. A good priority system should be able to adjust for these new issues and have some sense of which other issues can be given less attention instead, even if only for a short period. The unrest in the Middle East is an excellent example of the problem. The United States clearly had a stake in the stability of friendly Arab states, such as Tunisia and Egypt. This does not mean that analysts were blind to the negative aspects of the Zine Ben Ali and Hosni Mubarak governments. But there would be little reason, in late 2010, to give Tunisia the priority it likely assumed in early 2011 after the “Arab spring” revolts began. Egypt was already a nation of greater importance to U.S. national security. There was nothing in the decades that had passed in either country to suggest a sudden turn into instability, as opposed to the inevitability of a transfer of power at some unknown point as the autocrats aged.

Another issue in setting priorities is the fact that very few, if any, national security issues or threats are completely independent issues. Instead, there are interconnections among many issues. For example, the nexus between terrorism and weapons of mass destruction (WMD) is a constant concern. Terrorism is also connected to narcotics, as narcotics trafficking is a primary means of funding terrorism. In addition, terrorism and other transnational issues (crime, narcotics, human trafficking, etc.) thrive in failed states, which
have little law and order or control over their borders. The issues in such failed states are not equally important, or threatening, but it is necessary to take into account the interconnections when determining priorities. Thus, a lesser issue may get more attention because of its relationship to a more pressing issue. However, one cannot state that any issue that is related to a high-priority issue therefore also requires a high priority. If you did that, then almost every issue would end up with a relatively high priority, effectively undoing the entire priority system. One must recall the warning: “When everything is important, nothing is important.”

It is also important to understand that issues do not exist in an abstract realm: All issues have a geographic aspect. This may be broad or narrow, but every issue can be tied to specific locations. In determining priorities, it may be useful to differentiate based on the importance of the geographic aspect of the issue. For example, drugs being produced in Afghanistan may be seen as more problematic than those produced in Southeast Asia because of the Afghan–Taliban–al Qaeda connection. This geographic differentiation may also be useful in determining which supporting issues are more or less important.

Finally, issues are not monolithic. Every nation in which the United States has intelligence interests comprises several issues (e.g., political, military, social, economic) that will be of varying importance depending on the nation and its relationship to the United States. For example, U.S. interest in the state of the British military is that of assessing the capabilities of a close ally, while in North Korea we focus on the capabilities of a potential enemy. Although both are capabilities issues, the basis of our intelligence interest in each is quite different. Similarly, when dealing with a transnational issue, such as terrorists, it is important to differentiate among the various groups, their capabilities, their locations, and their interrelationships. Not every group will pose the same level of threat or of interest. It is important for intelligence managers to be able to make these distinctions to achieve the optimal allocation of both collection and analytical resources, even when examining the same issues.

Current Versus Long-Term Intelligence. The struggle between current and long-term intelligence is a perennial analytical issue. Current intelligence—reports and analysis on issues that may not extend more than a week or two into the future—is the mainstay of the intelligence community, the product most often requested and seen by policy makers. In many respects, current intelligence pays the rent for the intelligence community. Current intelligence always predominates over other types, but the degree of this predominance varies over time. During a crisis or war, current intelligence increases, as many of the decisions made during these periods are tactical in nature—even among senior policy makers—thus demanding current intelligence.
But some intelligence analysts are frustrated by the emphasis on current intelligence. Having developed expertise in an area and analytical skills, they wish to write longer range analyses that look beyond current demands. However, few policy makers are likely to read papers with very long time horizons—not owing to lack of interest but to lack of time and the inability to pull away, even briefly, from pressing matters. Thus, a conflict arises between what the policy makers need to read and what many analysts wish to produce. Current intelligence products also tend to be shorter by their nature and goals, further limiting the ability of analysts to add the depth or context that they deem valuable. An additional concern is that if current intelligence represents the majority of what analysts produce, then a risk arises that they will largely become reporters of that day’s collection instead of true analysts. Building true depth of expertise is difficult on a steady diet of current intelligence analysis.

Some middle ground exists simply because the intelligence community does not make a stark choice between one type of analysis and another on any given day. A range of analysis is produced. But because of the limited number of analysts, managers have to decide where to put their resources, and the fact remains that the current intelligence products predominate in terms of resources and the way policy makers perceive the intelligence community.

The current versus mid-term or long-term intelligence conundrum is not the only way to think about allocation issues, although it is the most common. Instead of thinking about intelligence as a matter of time, think about it as a depth versus breadth issue, or a tactical versus strategic issue. By its nature, most current intelligence tends to emphasize breadth over depth. However, one’s analytical sights can be raised to create intelligence that is current as well as strategic. Intelligence may be current in that it is focused on issues on the agenda right now or in the near future, but it also may attempt to give the policy maker a deeper look at the issues involved—for example, by providing more context, more interconnection with other issues or possible solutions, and so on. A more strategic current intelligence is not produced often, but it can be done without pushing the analysis into areas that policy makers are less likely to find useful.

The problem of current versus long-term intelligence also reflects yet another difference in outlook between policy makers and intelligence officers. Policy makers in the United States think in four-year blocks of time, the length of any presidential administration—which at best can be extended to eight years with reelection. Therefore, policy makers have difficulty thinking in larger blocks of time because of their more limited ability to influence events beyond their tenure. Another problem for long-term analytical products is the inherent “softness” of their judgments as their time frame increases. Trying to gauge likely conditions or outcomes is always difficult, but as the period...
being examined gets longer, the judgments become much less reliable. There is no absolute gauge about how far out analysis can be done and still be seen as reliable, but once the analysis ranges beyond a few years, the fidelity is likely to drop off markedly. Long-range analysis may be interesting intellectually, but it is unlikely to be seen as useful by policy makers. Indeed, it could even have a negative effect on the intelligence community at large if some policy makers question why resources are being devoted to this type of work rather than to more pressing and clearly identified issues that are on the current agenda.

**Briefings.** Briefings for policy makers are a form of current intelligence. Many are routine and take place first thing in the morning. Briefings are one of the main ways in which current intelligence is conveyed. One of the main advantages of briefings is the intelligence officer’s ability to interact directly with the policy maker, to get a better idea of the policy maker’s preferences and reactions to the intelligence, thus overcoming the absence of a formal feedback mechanism. Risks also are involved, though. Briefings, as their name indicates, tend to be brief. Given policy makers’ schedules, most briefings are limited by the time allotted for them. Moreover, the morning briefings usually must cover several topics—although both President George W. Bush and President Barack Obama have had regular in-depth briefings on a single issue, known as “deep dives.” Providing the necessary context and depth in a briefing can be difficult in a time-constrained environment.

At their best, briefings can be a give-and-take between the policy maker and the intelligence officer. This sort of exchange can be stimulating, but it runs risks. The briefer must be sure of his or her information, some of which may not be in the material that was prepared for the briefing. Briefers have to be taught to say, “I don’t know” and offer to get the desired information later, not hazard guesses. Furthermore, the briefing has an ephemeral quality. The briefer may not be able to recapture all that was said after the fact.

Briefings raise issues associated with analysts’ more proximate relationship with policy makers, particularly the ability to and necessity of keeping some distance from policy to maintain analytic objectivity. The regularly assigned briefers have a two-way role, conveying intelligence to the policy makers and conveying the policy makers’ needs or reactions back to the intelligence community. The briefers must avoid slipping into a role of advocacy or support for the policy makers’ policies, either writ large or in bureaucratic debates.

An area of controversy that arose in the aftermath of the terrorist attacks in 2001 was the nature of the Central Intelligence Agency (CIA) briefing for the president and senior officials. The briefing, which centers on the President’s Daily Brief (PDB), was a CIA publication, conducted exclusively by the CIA.
Although senior officials in the executive departments and in the intelligence community are privy to the PDB, this group is very small. Thus, other intelligence agencies do not necessarily know what the president or their own departmental policy makers are being told. This engenders a certain amount of jealousy and can lead to a situation in which analytic components of the intelligence community are working at cross-purposes.

In the aftermath of the passage of the 2004 intelligence legislation, control of the PDB shifted. The PDB staff became part of the Office of the Director of National Intelligence. For the CIA, control over the PDB was one of its crown jewels, giving it an assured level of access. However, responsibility for conducting the morning briefing has passed to the director of national intelligence (DNI). Under the DNI, the PDB is open to contributions from many analytical components. This makes it more of a community product and may also add greater breadth, but it highlights a problem in the DNI structure. When the DCI controlled the CIA and the PDB, the DCI had a greater sense of who was behind the PDB articles and, perhaps, a greater sense of ownership than the DNI. The DNI controls no analysts beyond the National Intelligence Council (NIC), so the DNI is, in effect, presenting the work of other agencies. In theory, and in law, the DNI has responsibility for all intelligence components but has authority over very few of them. Also, in terms of content, the CIA continues to be the main contributor to the PDB as it has the largest number of all-source analysts and thus the greatest depth and breadth of analytic capability, writ large.

Some believe that too much emphasis has been placed on the PDB, which has had a negative effect on overall analytic efforts. Spending time with the chief executive on a regular basis and being able to put an intelligence product before the president routinely are valuable assets. No intelligence manager would decline these opportunities. But decisions still have to be made about how much effort to put into preparing one discreet entity (the PDB) and how much goes into broader and perhaps deeper products. Analyses that go into the PDB or any other morning intelligence publication are non-urgent enough to wait until the next day. If the items reported on were crucial, they would be briefed to the president and other senior officials at once. This ongoing emphasis also skews the work of analysts, many of whom seek to write something that goes into the PDB or a deep dive, when this is hardly a significant indicator of analytic capability. An example of this overemphasis on the PDB is a result of the fact that other agencies may now contribute to it. In some intelligence agencies, managers set targets of how many PDB articles they should have in a given week or keep tallies of how many PDB articles their offices produced. Having an article in the PDB, while rewarding, is hardly a metric of analytic success.
**Crises Versus the Norm.** One way in which requirements are set is in response to crises. Crisis-driven requirements represent the ultimate victory of current over long-range intelligence needs.

Given the limited nature of collection and analytical resources, certain issues inevitably receive short shrift or even no attention at all. And, just as inevitably, annual or semiannual requirements planning regularly fails to predict which of the seemingly less important issues will erupt into a crisis. Thus, the planning exercises are to some degree self-fulfilling—or self-defeating—prophecies.

Analytical managers must find a way to create or preserve some minimal amount of expertise against the moment when a seemingly less important issue erupts and suddenly moves to the top of policy makers’ concerns. The intelligence community has only a small collection reserve, no analytical reserve, and a limited capacity to move assets to previously uncovered but now important topics. Assets therefore move from hot topic to hot topic, with other matters receiving little or no coverage.

Despite the problem of defining requirements and the vagaries of international relations, the intelligence community is on the spot when it misses an issue—that is, fails to be alert to its eventualty or is unprepared to deal with it when it occurs. In part, the high expectations are deserved, given that one function of intelligence is strategic warning. But strategic warning is usually taken to mean advance notice on issues that would pose a threat to national security, not regional crises that might require some level of involvement. Such crises strain the image of the intelligence community as well as its resources, because policy makers in both branches and the media tend to be harsh—sometimes fairly, sometimes not—in their view of misses.

One difficult aspect of dealing with crises that has arisen in recent years has been the demands of the combatant commanders (called COCOMs—the four-star officers who command U.S. forces in Europe, the Pacific, and so on) for intelligence support from national intelligence collection assets. The issue is one of conflicting priorities. The COCOMs are responsible for huge swaths of the globe and react to unrest in any of the countries in their area of responsibility (AOR). However, policy makers and intelligence officers in Washington, D.C., may not have the same sense of urgency about events in some of the smaller states and those that have less affiliation to the United States. Thus, there is a difference of perspective and perception. Efforts have been made to wean the COCOMs off their desire to call upon national assets for any and all emergencies in their AOR and to rely more on their own, admittedly less capable, theater intelligence assets.

The fact that the United States has been engaged in three hostile situations—terrorists, Iraq, and Afghanistan—tends to exacerbate the crises
versus the norm issue. Active combat or active intelligence operations tend to overwhelm other issues and activities. No one questions the importance of supporting either the military or intelligence operators, but these demands can become overwhelming, crowding out other issues. Also, for the intelligence community, a lot of these demands are tactical in nature, calling for support for an ongoing operation. This makes it more difficult for the intelligence analysts to “pull up to a higher altitude” and try to take a strategic view of the overall campaign. The war in Iraq has ended, and an active role in Afghanistan is coming to an end, but the fight against terrorists continues and may even expand geographically as the terrorists change their tactics and areas of operation. There is little reason to expect a significant decrease in emphasis on terrorism and related issues.

The Wheat Versus Chaff Problem. The wheat versus chaff problem, although part of collection, ultimately becomes an analytical issue. Although much that is collected does not get processed and exploited, the amount that does is still formidable. Even in the age of computers, few technical shortcuts have been found to help analysts deal with the problem. The intelligence community has adopted some software programs to assist in parts of information management, such as text mining and data mining, and has examined many others, but no major breakthroughs have been made. Thus, to a large degree, the analysts’ daily task of sifting through the incoming intelligence germane to their portfolios remains a grind, whether done electronically or on paper. Sifting is not just a matter of getting through the accumulated imagery, signals, open-source reporting, and other data. It is also the much more important matter of seeing this mass of material in its entirety, of being able to perceive patterns from day to day and reports that are anomalous. There are no shortcuts. Sifting requires training and experience. Although some intelligence practitioners think of analysts as the human in the loop, the analysts’ expertise should be an integral part of collection sorting as well.

Data Versus Knowledge. Closely related to the wheat versus chaff issue are the issues of data and of data versus knowledge. The ability to amass and manipulate large amounts of data on computers offers, to some, tantalizing possibilities for analysis and forecasting that did not exist before. There has been a great deal of discussion about big data, which in essence means the possibility of gaining new insights and connections from the reams of new data created every day. Part of the problem is in the counting rules. Most big data enthusiasts count all of the telephone calls, e-mails, tweets, blog posts, and so on created every day to prove how rich the field is. These data certainly exist, but how many of them are of interest or utility to intelligence analysts?
For example, of the millions of telephone metadata records searched by the National Security Agency (NSA), 300 led to further inquiries. The argument can be made that without the NSA metadata program these leads might not have existed at all, but a means-and-ends argument remains over the larger big data claims.

There are clearly intelligence issues that rely on large data inputs: the terrorism connections noted above, the details of weapons systems, or economic data. However, no amount of data will get at some of the key questions uppermost on the minds of policy makers: intentions. What North Korea or Iran or any other nation or leader will do next is not very susceptible to data. Moreover, as one senior policy official remarked, “I do not want data. I want knowledge and insight.”

There has also been some pushback on the utility of big data. As several analysts have noted, correlation, which is relatively easy with data, does not equal causation. (The Iraq WMD experience is a good illustration of this pitfall.) It is easy to confuse large amounts of data with in-depth knowledge and expertise. To a certain degree, data are much easier to deal with as they are almost mechanical and can give the illusion of useful insights when they actually may be somewhat ephemeral. As Kenneth Cukier and Viktor Mayer-Schoenberger noted in a 2013 article in Foreign Affairs: “Big data is a resource and a tool. It is meant to inform, rather than explain.”

Analytical managers will therefore have to be on guard to assure themselves that their analysts also continue to be “knowledge workers,” a term coined by Peter Drucker around 1959 to connote someone who works primarily with information or who develops and uses knowledge in the workplace. Indeed, one of the main functions of the intelligence community in the past had been the creation, preservation, and transmission of knowledge. Some argue that this function has atrophied as analysts and managers focus more on data and as the overall experience level within the intelligence community has declined in the years since 2001 as senior analysts retired and there was also a huge influx of new analysts.

**Analyst Fungibility.** When requirements change or when crises break out, analysts must be shifted to areas of greater need. As with collection, they are participating in a zero-sum game. The analysts have to come from some other assignment, and not every analyst can work on every issue. Each analyst has strengths, weaknesses, and areas that he or she simply does not know. Even though analysts far outnumber collection systems, analysts are less fungible—that is, easily interchanged or replaced—than the technical collection systems. A signals intelligence satellite that has been collecting against a French-speaking target will not plead ignorance or inability if redirected against an
Arabic-speaking target. Significant issues of targeting, access, frequencies, and so on come up, but no language barrier exists per se. Streams of digital communications data do not have indecipherable accents. However, not every analyst has the requisite language, regional, or topical skills to move to an area of greater need. Very real limits exist on analyst fungibility, which is a major management concern. This is also sometimes referred to as analyst agility, again meaning the need for analysts who have more than one (or two) areas of expertise and therefore can be shifted to higher priority accounts during times of need. Fungibility or agility relies on three factors: the talents and background of the analysts when they are recruited; their training and education within the intelligence community; and the management of their careers, which should give them sufficient opportunities to develop this expertise in a few areas.

U.S. intelligence managers often speak about global coverage, which can be a dangerous and misleading term. By global coverage, intelligence officers mean their acknowledged requirement to cover any and all issues. Members of the intelligence community cannot say to a policy maker, for example, that they do not have much capability to analyze the current crisis in Mali but they are very good on Mexico. No bait and switch is allowed. If the situation in a country or region becomes a matter of concern, the intelligence community is expected to cover it. The pitfall in the term “global coverage” is the real possibility that it leaves the impression among policy makers of more depth and breadth than is available in the intelligence community. Intelligence managers understand the resource limitations within which they are working, but by using the term global coverage they may be misinterpreted as promising more than they can deliver.

Part of the problem stems from the limitations of the analyst hiring process. In the United States, recruiters go to colleges and universities looking for potential analysts. Other candidates simply apply on their own. But this is a seller’s market. The intelligence agencies can hire only those people who evince an interest. Certain schools may have programs that tend to produce more analysts of a certain interest or skill, but this does not appreciably solve the problem. Congress has given the intelligence community a limited ability to offer scholarships for analysts with particular skills, in return for which the analysts must work for the intelligence community for a set number of years. Although a valuable change, such ability does not solve the recruitment problem. It is also very difficult to forecast analytical needs several years out. Analysts tend to be hired against current needs in terms of skill sets, areas of expertise, and languages. This can create imbalances when issues shift dramatically. For example, the Soviet Union remained a priority until its collapse, but once it was gone there was a surplus of Russian language
speakers, not all of whom could easily be shifted to other issues. Similarly, in the aftermath of the terrorist attacks in 2001, there was an urgent and very difficult-to-fill need for speakers and readers of Arabic and then for the many non-Roman alphabet languages spoken in southwestern Asia.

Thus, the intelligence community has greater analytic capabilities in some areas than in others. The situation can be ameliorated to some extent by moving analysts around from issue to issue, but sacrificing depth for breadth can result. Moreover, during a crisis, what is wanted most from analysts is depth. The point remains that all analysts have limitations that can curtail the ability of the intelligence community to respond as expected and as the community would prefer.

**Analyst Training.** The intelligence community’s approach to training has been somewhat idiosyncratic, with each major component creating unique training programs. Training is most useful in giving incoming analysts a sense of what is expected of them, how the larger community works, and its ethos and rules. No amount of training, however, can obviate the fact that much of what an analyst needs to know is learned on the job. Analysts arrive with certain skills garnered from their college or graduate school studies or their work experience (a significant number of analysts now come to the intelligence community after having begun careers in other areas) and then are assimilated into their specific intelligence agency or unit. They learn basic processes and requirements, the daily work schedule, and preferred means of expression, which vary from agency to agency. They become familiar with the types of intelligence with which they will be working.

The minimum skills for all analysts are knowledge of one or more specific fields, appropriate language skills, and a basic ability to express themselves in writing. A senior official used to ask his subordinates two questions about new analysts they wished to hire: Do they think interesting thoughts? Do they write well? This official believed that, with these two talents in hand, all else would follow with training and experience.

The basic skills are a foundation on which better skills must be built. Some of the new skills to be mastered are parochial. Each intelligence agency has its own corporate style that must be learned. More important, analysts must learn to cope with the wheat versus chaff problem and to write as succinctly as possible. These two skills reflect the demands of current intelligence and the fact that policy makers are busy and prefer economies of style. The bureaucratic truism remains that shorter papers will usually best longer papers in the competition for policy makers’ attention.

Training analysts about collection systems appears to fall short of desired goals, given the ignorance expressed by even some senior analysts about this
important topic. This means that some analysts are hard put to understand the true nature and relative reliability of intelligence sources because they do not have a very deep appreciation of how they are collected. This does not mean that every analyst has to be deeply versed in each of the collection disciplines, but something more than a superficial knowledge is an analytical advantage. Another important skill that analysts must learn is objectivity. Although intelligence analysts can and often do have strong personal views about the issues they are covering, their opinions have no place in intelligence products. Analysts are listened to because of their accumulated expertise, not the forcefulness of their views. Presenting personal conclusions would cross the line between intelligence and policy. Still, analysts need training to learn how to filter out their views, especially when they run counter to the intelligence at hand or the policies being considered.

A more subtle and difficult skill to master is cultivating the intelligence consumer without politicizing the intelligence as a means of currying favor.

Finally, there is the question of how far training (or experience) can take a given analyst. Any reasonably intelligent individual with the right skills and education can be taught to be an effective analyst. But the truly gifted analyst—like the truly gifted athlete, musician, or scientist—is inherently better at his or her job by virtue of inborn talents. Being able to analyze and synthesize intuitively and quickly and having a good nose for the subtext of a situation are innate skills that are hard to acquire. In all fields, such individuals are rare. They must be nurtured. But the benefits they derive from training are different from those that accrue to less gifted analysts.

Part of the underlying problem in analyst education and training has been the rather vague sense across the intelligence community of what an analyst’s career progression of skills should look like. There has been some general agreement, but it has not been specific enough or accepted across all agencies. It is extremely difficult to create an education program if the levels of achievement are not described with some precision. A recent, more detailed effort by the CIA’s Sherman Kent School has been the intelligence analyst training program, which describes the skills required at progressive levels: 1st year: career analyst program; 1+ years: essential skills; 4+ years: advanced analyst; 10+ years: expert.

Managing Analysts. Managing intelligence analysts presents a number of unique problems. A major concern is developing career tracks. Analysts need time to develop true expertise in their fields, but intellectual stagnation can set in if an analyst is left to cover the same issue for too long. Rotating analysts among assignments quickly helps them avoid becoming stale and allows them to learn more than one area. But this career pattern raises the possibility
that analysts will never gain expertise in any one area, instead becoming generalists. Ideally, managers seek to create some middle ground—providing analysts with assignments that are long enough for them to gain expertise and substantive knowledge while also providing sufficient opportunities to shift assignments and maintain intellectual freshness. Nor is there any specific time frame for assignments; the length depends on the individual analyst, the relative intensity of the current assignment, and the demands generated by intelligence requirements at the time. More intense jobs tend to argue for somewhat shorter tours to avoid burnout. But more urgent issues also tend to have higher priority, demanding greater expertise and consistency of staffing. Thus, there are again competing needs.

The criteria for promotion are another management issue. As government employees, intelligence analysts are generally assured of promotions up to a level that can be described as high-middle. The criteria for promotion through the grades are not overly rigorous. Promotions should come as a result of merit, not time served. But what criteria should a manager consider in evaluating an intelligence analyst for merit promotion: accuracy of analysis over the past year, writing skills, increased competence in foreign languages and foreign area knowledge, participation in a specific number of major studies, intellectual growth in mastering new areas? And how should a manager weigh the various criteria?

The competition is stronger for more senior assignments than for those at the lower level, and the criteria for selection are different. The qualities that first merit promotion—keen analytical abilities—are the ticket to management positions, where responsibilities and pay are greater. Ironically, or perhaps sadly, analytical skills have little to do with, and are little indication of, the ability to carry out managerial duties. But, with few exceptions, management positions have been the only route to senior promotion. The CIA has created a Senior Analytical Service, which allows analysts to reach the first rungs of senior ranks solely on the basis of their analytical capabilities.

**Analysts’ Mind-Set.** Analysts, as a group, exhibit a set of behaviors that can affect their work. Not all analysts exhibit each of these characteristics all of the time, and some analysts may never display any of them. Still, many of these traits are common among this population.

One of the most frequent flaws of analysts is mirror imaging, which, as described earlier, assumes that other leaders, states, and groups share motivations or goals similar to those most familiar to the analyst. “They’re just like us” is the quintessential expression of this view. The prevalence of mirror imaging is not difficult to understand. People learn, from an early age, to expect certain behavior of others. The golden rule is based on the concept
of reciprocal motives and behavior. Unfortunately, as an analytical tool, mirror imaging fails to take into account such matters as differences of motivation, perception, or action based on national differences, subtle differences of circumstance, different rationales, and the absence of any rationale.

Simon Montefiore (Stalin: The Court of the Red Tsar) quotes Josef Stalin as saying, “When you’re trying to make a decision, NEVER put yourself in the mind of the other person because if you do, you can make a terrible mistake.” For example, during the cold war, some Kremlinologists and Sovietologists talked about Soviet hawks and doves and tried to assess which Soviet leaders belonged to which group. No empirical evidence existed to suggest that there were Soviet hawks and doves. Instead, the fact that the U.S. political spectrum included hawks and doves led to the facile assumption that the Soviet system must have them as well. More recently, some commentators and analysts working on Iran speak of Iranian extremists and moderates. When pressed by skeptical peers as to their evidence for the existence of moderates, the response is often this: If there are extremists, there must be moderates. Again, they reflect other political systems they know as well as making a faulty assumption. It could be argued that in Iranian politics there are ultra-extremists and extremists, but that someone who is considered moderate within the context of Tehran might not fit that definition in the wider world.

To avoid mirror imaging, managers must train analysts to recognize it when it intrudes in their work and must establish a higher level review process that is alert to this tendency.

Clientism is a flaw that occurs when analysts become so immersed in their subjects—usually after working on an issue for too long—that they lose their ability to view issues with the necessary criticality. (In the State Department this phenomenon is called “clientitis,” which should be defined as “an inflammation of the client,” although the term is used when referring to someone who has “gone native” in his or her thinking.) Analysts can spend time apologizing for the actions of the nations they cover instead of analyzing them. The same safeguards that analysts and their managers put in place to avoid mirror imaging are required to avoid clientism.

The issue of “layering” arose largely as a result of the Iraq WMD experience. Layering refers to the use of judgments or assumptions made in one analysis as the factual basis for judgments in another analysis without also carrying over the uncertainties that may be involved. This can be especially dangerous if the earlier judgments were based on meager collection sources. Analysts are allowed—and are expected—to make assumptions; they are not allowed to use these assumptions as the factual basis for additional assumptions. Layering tends to give these earlier judgments greater certainty and can mislead analysts and, more important, policy makers. Both the
Senate Intelligence Committee and the WMD Commission (Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction) accused intelligence analysts of layering when they analyzed Iraq’s alleged possession of WMD.

Finally, there is the issue of linear thinking. Most people think linearly since most days pretty much resemble those days before and after. Thus, it is easy for linearity to creep into analysis. The problem is that analysts need to be constantly on the watch for discontinuities, for nonlinear events. This is a fairly constant requirement, albeit a difficult one. An analyst has to walk a fine line between being blasé and being a doomsayer. However, it is the discontinuities that prove to be most problematic for policy makers. The collapse of the Soviet Union, the crisis of the Euro in 2010–2011, or the so-called Arab Spring are all good examples of nonlinear events. Baseball icon Yogi Berra was correct when he said, “The future will be just like the past, only different.” A good analyst should look at the issues in his or her brief and constantly ask, “What might arise to put this on a different path?” The chances of coming up with the precisely right answer may be small, but the questions help counter linearity and complacency.

**On-the-Ground Knowledge.** Analysts have varying degrees of direct knowledge about the nations on which they write. During the cold war, U.S. analysts had difficulty spending significant amounts of time in the Soviet Union or its satellites, and they were unable to travel widely in those nations. Similarly, intelligence analysts may have less contact with the senior foreign officials about whom they write than do the U.S. policy makers who must deal with these foreigners. Analysts’ distance from the subjects being analyzed can occasionally be costly in terms of how their policy consumers view the intelligence they receive. Some policy clients also may have more in-country experience than do the intelligence analysts.

This problem can be compounded when dealing with terrorists, with whom few opportunities arise for direct or prolonged contact and perhaps little shared basis of rationality by which to gauge their motives or likely next actions. Recent studies of intelligence analysis by then-Maj. Gen. Michael Flynn in Afghanistan and by former National Security Council (NSC) Asia director Kenneth Lieberthal offer the same critique about the paucity of on-the-ground knowledge and on the effects this has on policy and how policy makers view intelligence.

Analysts, like everyone else, are proud of their accomplishments. Once they have mastered a body of knowledge, they may look for opportunities—no matter how inappropriate—to display that knowledge in detail. Analysts can have difficulty limiting their writing to those facts and analyses that
may be necessary for a specific consumer need. Analysts may want the consumer to have a greater appreciation for where the issues being discussed fit in some wider pattern. Unfortunately—and perhaps too frequently—the policy client wants to know “only about the miracles, and not the lives of all the saints who made them happen.” Analysts require training, maturity, and supervision to cure this behavior. Some analysts get the message sooner than others; some never get it and produce analysis that requires greater editing to get to the essential message, which can cause resentment on the part of either analysts or their editors. Furthermore, the intelligence provider may lose the attention of the policy client if he or she gives too much material, large portions of which do not seem relevant to the policy maker’s immediate needs.

Just as analysts want to show the depth of their knowledge, so, too, they want to be perceived as experienced—perhaps far beyond what is true. Again, this is a common human failing. Professionals in almost any field, when surrounded by peers and facing a situation that is new to them but not to others, are tempted to assert their familiarity, whether genuine or not. Given the choice between appearing jaded ("been there, done that") and naive ("Wow! I’ve never seen that before!"), analysts usually choose jaded. The risk of being caught seems small enough, and it is preferable to being put down by someone else who displays greater experience.

Sometimes, however, much is at stake. For example, in April 1986 the operators of the Chernobyl nuclear reactor in the Soviet Union, while running an unauthorized experiment, caused a catastrophic explosion. The next afternoon, Sweden reported higher than normal radioactive traces in its air monitors, which had been placed in many cities. In the United States, an intelligence manager asked a senior analyst what he made of the Swedish complaints. The analyst played them down, saying the Swedes were always concerned about their air and often made such complaints for the smallest amounts of radiation. On discovering what was actually going on, analysts spent the following day frantically trying to catch up with the facts about Chernobyl. The jaded approach precluded the analysts from making the simplest inquiries, such as what types of radiation Sweden detected. The answer would have identified the source as a reactor and not a weapon. And the prevailing winds over Sweden could have been surveyed to identify the source. (Some years later the intelligence manager met with some of his Swedish counterparts. They had initially concluded, based on analysis of the radiation and wind conditions, that a reactor at nearby Ignalina, across the Baltic Sea in Soviet territory, was leaking. Although they misidentified the source, which was a reactor much farther away, they were much closer to the truth than were U.S. intelligence officials.)
The costs of the jaded approach are threefold. First, this approach represents intellectual dishonesty, something all analysts should avoid. Second, it proceeds from the false assumption that each incident is much like others, which may be true at some superficial level but may be false at fundamental levels. Third, it closes the analyst’s thinking, regardless of his or her level of experience, to the possibility that an incident or issue is entirely new, requiring wholly new types of analysis.

Credibility is one of the most highly prized possessions of analysts. Although they recognize that no one can be correct all of the time, they are concerned that policy makers are holding them accountable to an impossible standard. Their concern about credibility—which is largely faith and trust in the integrity of the intelligence process and in the ability of the analysts whose product is at hand—can lead them to play down or perhaps mask sudden shifts in analyses or conclusions. For example, suppose intelligence analysis has long estimated a production rate of fifteen missiles a year in a hostile state. One year, because of improved collection and new methodologies, the estimated production rate (which is still just an estimate) goes to forty-five missiles per year. Policy makers may view this increase—on the order of 300 percent—with alarm. Instead of presenting the new number with an explanation as to how it was derived, an analyst might be tempted to soften the blow. Perhaps a brief memo is issued, suggesting changes in production. Then a second memo, saying that the rate is more likely twenty to twenty-five missiles per year, and so on, until the policy maker sees a more acceptable analytical progression to the new number and not a sudden spike upward. Playing out such a scenario takes time, and it is intellectually dishonest.

Intelligence products that are written on a recurring basis—such as certain types of national intelligence estimates—may be more susceptible than other products to this type of behavior. They establish benchmarks that can be reviewed more easily than, say, a memo that is not likely to be remembered unless the issue is extremely important and the shift is dramatic.

At the same time, there are risks inherent in sudden and dramatic shifts in analysis. In November 2007, DNI Mike McConnell (2007–2009) released unclassified key judgments of a new national intelligence estimate (NIE) on Iran’s nuclear intentions and capabilities. The NIE estimated that Iran had ceased its weaponization program in 2003, reversing views held in a 2005 estimate. Officials explained that recently collected intelligence had led to the new position. But observers and commentators questioned why this had not been known earlier, failing to understand the nature of intelligence collection. Some wondered if the new conclusions were “compensation” (or penance) for the mistaken conclusions in the 2002 Iraq WMD estimate. And some wondered if the intelligence community was trying to prevent the Bush
administration from using force against a recalcitrant Iran. Interestingly, few commentators took the NIE at face value, accepting the possibility that analytic views had changed.

Although policy makers have taken retribution on analysts for sudden changes in estimates, more often than not the fear in the minds of analysts is greater than the likelihood of a loss of credibility. Much depends on the prior nature of the relationship between the analyst and the policy maker, the latter’s appreciation for the nature of the intelligence problem, and the intelligence community’s past record. If several revisions have been made in the recent past, there is reason to suspect a problem. If revision is an isolated phenomenon, it is less problematic. The nature of the issue, and its importance to the policy maker and the nation, also matters.

For example, the level of Soviet defense spending—then usually expressed as a percentage of gross national product (GNP)—was a key intelligence issue during the cold war. At the end of the Gerald Ford administration (1974–1977), intelligence estimates of Soviet GNP going to defense rose from a range of 6 to 7 percent to 13 to 14 percent, largely because of new data, new modeling techniques, and other factors unrelated to Soviet output. The revision was discomfiting to the incoming Jimmy Carter administration. In his inaugural address, Carter signaled that he did not want to be constantly concerned with the Soviet issue, that he had other foreign policy issues to pursue. A more heavily armed Soviet Union was not good news. Carter prided himself on his analytical capabilities. When faced with the revised estimates, he reportedly chided the intelligence community, noting that they had just admitted to a 100 percent error in past estimates. That being the case, why should he believe the latest analyses?

Few intelligence products are written by just one analyst and then sent along to the policy client. Most have peer reviews and managerial reviews and probably the input of analysts from other offices or agencies. This is especially true for the intelligence products (analytical reports) that agencies call estimates in the United States or assessments in Australia and Britain. Participation of other analysts and agencies adds another dimension to the analytical process—bureaucratics—which brings various types of behaviors and strategies.

More likely than not, several agencies have strongly held and diametrically opposed views on key issues within an estimate. How should these be dealt with? The U.S. system in both intelligence and policy making is consensual. No votes are taken; no lone wolves are cast out or beaten to the ground. Everyone must find some way to agree. But if intellectual arguments fail, consensus can be reached in many other ways, few of which have anything to do with analysis.

• Back scratching and logrolling. Although usually thought of in legislative terms, these two behaviors can come into play in
intelligence analysis. Basically, they involve a trade-off: “You accept my view on p. 15 and I’ll accept yours on p. 38.” Substance is not a major concern.

- False hostages. Agency A is opposed to a position being taken by Agency B but is afraid its own views will not prevail. Agency A can stake out a false position on another issue that it defends strongly, not for the sake of the issue itself, but so that it has something to trade in the back scratching and logrolling.

- Lowest common denominator language. One agency believes that the chance of something happening is high; another thinks it is low. Unless these views are strongly held, the agencies may compromise—a moderate chance—as a means of resolving the issue. This example is a bit extreme, but it captures the essence of the behavior—an attempt to paper over differences with words that everyone can accept.

- Footnote wars. Sometimes none of the other techniques works. In the U.S. estimative process, an agency can always add a “footnote” in which it expresses alternative views. (In estimates, these are not actually footnotes, that is, text at the very bottom of the page. They are successive paragraphs in the main text that express alternate views but are flagged as not being the majority or consensus opinion.) Or more than one agency might add a footnote, or agencies may take sides on an issue. This can lead to vigorous debates as to whose view appears in the main text and whose in the footnote.

In U.S. practice, an estimate may refer to “a majority of agencies” or a “minority.” This is an odd formulation. First, it is vague. How many agencies hold one view or the other? Is it a substantial majority (say, eleven of the sixteen agencies) or a bare one? Second, the formulation strongly implies that the view held by the majority of agencies is more likely the correct one, although no formal or informal votes are taken in the NIE process. The British practice is different. In Britain, if all agencies participating in an assessment cannot agree, then the views of each are simply laid out. This may be more frustrating for the policy maker reading the assessment, but it avoids false impressions about consensus or correct views based on the vague intellectual notion of a majority.

One critique of the intelligence community’s analysis of Iraq WMD was the absence of different views and the problem of groupthink. The Senate Intelligence Committee held that the analysts did not examine their assumptions rigorously enough and thus lapsed too easily into agreement. The case highlights a conundrum for managers and analysts, particularly those involved in estimates. As a rule, policy makers prefer consensus views, which
save them from having to go through numerous shades of opinion on their own. After all, isn’t that what the intelligence community is supposed to be doing? Thus, there has always been some impetus to arrive at a consensus, if possible. In the aftermath of Iraq, however, most consensus views—even if arrived at out of genuine agreement—could be viewed with suspicion. How does one determine, when reading intelligence analysis, the basis on which a consensus has been achieved? How does one determine if it is a true meeting of minds or some bureaucratic lowest common denominator?

**Analytical Stovepipes.** Collection stovepipes emerge because the separate collection disciplines are often based on different technologies, are managed independently, and often are rivals to one another. Analytical stovepipes also appear in the U.S. all-source community. The three all-source analytical groups—the CIA’s Directorate of Intelligence, Defense Intelligence Agency’s Directorate of Intelligence, and the State Department’s Bureau of Intelligence and Research (INR)—exist to serve specific policy makers. They also come together on a variety of community analyses, most often the NIEs. Efforts to manage or, even more minimally, to oversee and coordinate their activities reveal a stovepipe mentality not unlike that exhibited by the collection agencies. The three all-source agencies tend to have a wary view of efforts by officials with community-wide responsibilities to deal with them as linked parts of a greater analytical whole. The analytical agencies manifest this behavior less overtly than do the collectors, so it is more difficult to recognize. It thus may be surprising to some people, perhaps more so than when collectors exhibit this behavior. After all, each of the collectors operates in a unique field, with a series of methodologies that are also unique. The analytical agencies, however, are all in the same line of work, often concerned with the same issues. But bureaucratic imperatives and a clear preference for their responsibilities in direct support of their particular policy clients, as opposed to interagency projects, contribute to analytical stovepipes.

All of these behaviors can leave the impression that the estimative process—or any large-group analytical efforts—is false intellectually. That is not so. However, it is important to note that intelligence analysis is not a purely academic exercise. Other behaviors intrude, and more than just analytical truths are at stake. The estimative process yields winners and losers, analysts whose papers go forward and those whose do not, and careers may rise and fall as a result.

**Analytical Issues**

In addition to the mind-set and behavioral characteristics of analysts, several issues within analysis need to be addressed.
**Competitive Versus Collaborative Analysis.** As important as the concept of competitive analysis is to U.S. intelligence, a need has been seen to bring together analysts of agencies or disciplines to work on major ongoing issues, in addition to the collaborative process of NIEs. DCI Robert M. Gates (1991–1993) created centers, most of which focused on transnational issues—terrorism, nonproliferation, narcotics, and so on.

The intelligence community also forms task forces to deal with certain issues; among these was the Balkans task force, which has operated since the 1990s, monitoring the range of issues related to the breakup of Yugoslavia.

The 9/11 Commission (National Commission on Terrorist Attacks upon the United States) recommended organizing all analysis around either regional or functional centers. The 2004 intelligence law mandated the establishment of the National Counterterrorism Center (NCTC), which was basically an expansion of the Terrorism Threat Integration Center that DCI George J. Tenet (1997–2004) had created. The law also required that the DNI examine the utility of creating a National Counterproliferation Center, which was done, and gives the DNI the authority to create other centers as necessary. The problem with the center approach for all analysis is that it becomes somewhat inflexible. Inevitably, some issues or some nations do not fit easily into the center construct. What happens to them? Also, although creating a center is easy, centers—like all other offices—do not like to share or lose resources. Centers therefore run counter to the desire for analytic workforce agility. To date, centers have been organized along functional lines and are staffed by analysts who tend to be more expert in the issue than in the national or regional context within which that issue has been raised. A functional center therefore runs the risk of providing technical analysis that is divorced from its political or cultural context. For example, analyzing the state of WMD development in a nation is not enough. One should also analyze the internal or regional political factors driving the program, as these will give important indicators as to its purpose and scope. Being housed in a center does not preclude a functional analyst from seeking out his or her regional counterparts. Analysts do this on a regular basis. But it requires some effort and can be dropped during the press of the day’s work. The center concept can serve to make collaboration beyond the bounds of the center itself more difficult.

Centers can become competitors for resources with offices in agencies. This appears to have been the case with the NCTC and CIA’s Counterterrorism Center, according to the WMD Commission. As has been seen from the time that DCI Gates began creating centers in the early 1990s, the heads of agencies are not willing to siphon away scarce resources to an activity over which they will have no control (centers fell under the jurisdiction of the DCI and now are under the DNI) and from which they will receive no direct results. The
WMD Commission recommended the creation of an additional center, the National Counterproliferation Center, which has a managerial role in line with the commission’s concept of mission managers to coordinate collection and analysis on specific issues or topics.

A bureaucratic debate has ensued on the nature of the centers. Although their goal is to bring the intelligence components into a single place, most centers had been located in and dominated by the CIA. Some people argue that the arrangement undercuts the centers’ basic goal—to reach across agencies. Defenders of the system argue that housing the centers in the CIA gives them access to many resources not available elsewhere and also protects their budgets and staffing. A 1996 review by the House Intelligence Committee staff validated the concept of the centers but urged that they be less CIA-centric. Given the location of the centers, however, other agencies are sometimes loath to assign analysts to them, fearing that they will be essentially lost resources during their center service. (A similar problem used to occur on the Joint Staff, which supports the Joint Chiefs of Staff. The military services—Army, Navy, Air Force, Marines—naturally preferred to keep their best officers in duties directly related to their service. This ended when Congress passed the Goldwater-Nichols Act in 1986, which mandated a joint service tour as a prerequisite for promotion to general or admiral.) Intelligence community centers (as opposed to centers that are still created by and housed in individual agencies) now are overseen by the DNI, which should serve to make the centers more community based in terms of staffing. However, the setup raises new issues about how the DNI staffs the centers when he or she has no direct control over any analytic components comparable to the control that the DCI had over the CIA. DNI McConnell created the requirement that intelligence officers have “joint duty” assignments before being promoted to senior ranks (similar to the requirement for the military) to make assignments to centers more attractive, especially for one’s most talented officers, as a means of assuring their continued promotion. Another issue for the centers is their longevity. In government—in all sectors—ostensibly temporary bodies have a way of becoming permanent, even when the reasons for their creation have long since ended. A certain bureaucratic inertia sets in. Some people wish to see the body continue, as it is a source of power; others fear that by being the first to suggest terminating it they will look like shirkers. The situation has a comic aspect to it, but also a serious one, as these temporary groups absorb substantial amounts of resources and energy.

Thus, the question for the centers—or any other groups—is this: When are they no longer needed? Clearly, the transnational issues are ongoing, but even they may change or diminish over time. One former deputy DCI suggested a five-year sunset provision for all centers, meaning that every five years
each center would be subject to a hard-nosed review of its functions and the requirement for its continuation.

Finally, some critics question the focus of the centers, arguing that they are concentrating tactically on operational aspects of specific issues instead of on the longer term trends. Center proponents note the presence of analysts and the working relationship between the centers and the national intelligence officers (NIOs), who can keep apprised of the centers’ work, offer advice, and are responsible for the production of NIEs.

The WMD Commission, reporting in March 2005, recommended the creation of mission managers to “ensure a strategic, Community-level focus on priority intelligence missions.” The commission envisioned these managers overseeing both collection and analysis on a given issue, as well as fostering alternative analyses on their issue. However, the mission managers would not conduct actual analysis; rather, they would facilitate analysis. The commission also posited that the mission managers offered a more flexible approach than the centers. The commission recommended that mission managers oversee target development and research and development for their issues. In 2010, DNI James Clapper stated that the mission manager system and the NIO system (each supposedly being the lead analyst for his or her area) created either confusion or redundancy. Still concerned about achieving better integration between collection and analysis—indeed, this became the main theme of his tenure—Clapper decided to merge the two functions. Under Clapper there are now national intelligence managers (NIMs), whose portfolios largely reflect the NIO’s portfolios.

As of 2013, there were fifteen NIMs: seven regional (Africa, East Asia, Eurasia, Near East, South Asia, Western Hemisphere, Iran) and eight transnational (Counterterrorism, Counterproliferation, Counterintelligence, Cyber, Economics, Military Issues, Science and Technology, Threat Finance). The Department of Homeland Security (DHS) had asked for a NIM for Homeland Security, which DNI Clapper refused. A Deputy NIM for Homeland Security was created, under the NIM for the Western Hemisphere. The NIM concept raises several issues, as did the mission managers. First, and most obvious, is their authority to target collection or facilitate analysis. These activities occur in the various intelligence agencies, where the DNI faces very real limits to his or her authority, as did the DCI. Second, it is exceedingly difficult for managers to maintain awareness of all of the analysis being produced on certain issues. The NIMs must also have knowledge of the analysts working on an issue across the community. Here the DNI has benefited from the Analytic Resources Catalog (ARC), a listing of all analysts and their subject area and past expertise, which was created under DCI Tenet. Annually, each NIM is expected to write a “State of the Mission” letter.
to the DNI, discussing how integration and other issues are progressing in their mission. Finally, creation of the NIMs led to questions about their roles versus that of the NIOs, which appear to be similar in some respects. The NIOs had been seen as the intellectual leaders for their issues in the intelligence community, and they had some sense of lost status vis-à-vis the NIMs, especially as each NIO is part of the NIM team as the analytical expert. (There is also a national intelligence collection officer—NICO—and a national counterintelligence officer—NCIO—on each NIM team.)

Ultimately, there is no best way to organize analysts. Each scheme has distinct advantages and disadvantages. Each scheme still revolves around either functional or regional analysts. The goal should be to ensure that the right analysts of both types are brought to bear on topics as needed, either on a permanent or temporary basis, depending on the issue and its importance. Flexibility and agility remain crucial. (See box, “Metaphors for Thinking About Analysis.”)

Metaphors for Thinking About Analysis

Metaphors are often used to describe the intelligence analysis process. Thomas Hughes, a former director of the Department of State Bureau of Intelligence and Research, wrote that intelligence analysts were either butchers or bakers. Butchers tend to cut up and dissect intelligence to determine what is happening. Bakers tend to blend analysis together to get the bigger picture. Analysts assume both roles at different times. In the aftermath of the September 11 terrorist attacks, the phrase “connect the dots” became prevalent as a means of describing an analytic intelligence failure. It is an inapt metaphor. Connecting the dots depends on all of the dots being present to draw the right picture. (The dots also come numbered sequentially, which helps considerably.) As a senior intelligence analyst pointed out, the intelligence community was accused of not connecting the dots in the run-up to September 11 but was accused of connecting too many dots regarding the alleged Iraqi weapons of mass destruction. Two more useful descriptions are mosaics or pearls. Intelligence analysis is similar to assembling a mosaic, but one in which the desired final picture may not be clear. Not all of the mosaic pieces may be available. Further complicating matters, in the course of assembling the mosaic, new pieces appear and some old ones change size, shape, and color. The pearl metaphor refers to (Continued)
how intelligence is collected and then analyzed. Most intelligence issues are concerns for years or even decades. Like the slow growth of a pearl within an oyster, there is a steady aggregation of collected intelligence over time, allowing analysts to gain greater insight into the nature of the problem. Why do these metaphors matter? They matter because they will affect how one views the analytical process and the expectations one has for the outcomes of that process.

**Dealing With Limited Information.** Analysts rarely have the luxury of knowing everything they wish to know about a topic. In some cases, little may be known. How does an analyst deal with this problem?

One option is to flag the problem so that the policy client is aware of it. Often, informing policy consumers of what intelligence officials do not know is as important as communicating what they do know. Secretary of State Colin Powell (2001–2005) used the formulation: “Tell me what you know. Tell me what you don’t know. Tell me what you think.” Powell went on to say that he held intelligence officers responsible for what they knew or did not know but that he was responsible if he took action based on what they think. But admitting ignorance may be unattractive, out of concern that it will be interpreted as a failing on the part of the intelligence apparatus. Alternatively, analysts can try to work around the problem, utilizing their own experience and skill to fill in the blanks as best they can. This may be more satisfying intellectually and professionally, but it runs the risk of giving the client a false sense of the basis of the analysis or of the analysis being wrong.

Another option is to arrange for more collection, time permitting. Yet another is to widen the circle of analysts working on the problem to get the benefit of their views and experience.

A reverse formulation of this same problem has arisen in recent years. To what degree should analysis be tied to available intelligence? Should intelligence analyze only what is known, or should analysts delve into issues or areas that may be currently active but for which no intelligence is available? Proponents argue that the absence of intelligence does not mean that an activity is not happening, only that the intelligence about it is not available. Opponents argue that this sort of analysis puts intelligence out on a limb, where there is no support and the likely outcome is highly speculative worst-case analysis. On the one hand, intelligence analysis is not a legal process in which findings must be based on evidence. On the other hand, analysis written largely on supposition is not likely to be convincing to many and may be more susceptible to politicization.
For many years, the intelligence community has stressed the importance of analytic penetration, as an intellectual means of trying to overcome a dearth of intelligence sources. Analytic penetration means thinking longer and harder about the issue, perhaps making suppositions of what is most likely, and perhaps laying out a range of outcomes based on a set of reasonable assumptions. The underlying premise in analytic penetration is that the analytic community does not have the luxury of simply throwing up its hands and saying, “Sorry, no incoming intelligence; no analysis.” But if analysis is required and the sources are insufficient, there has to be rigor applied to the analysis that attempts to make up for these missing sources. This is an area where greater collaboration across offices and agencies would be most useful.

The concerns about dealing with limited intelligence arose in the reviews of intelligence performance before the 2001 terrorist attacks and the intelligence before the Iraq war (2003–2011). The problems in each case were different. In the case of the September 11 attacks, some people criticized analysts for not putting together intelligence they did have to get a better sense of the al Qaeda threat and plans. Intelligence officials were also criticized for not being more strident in their warnings—a charge that intelligence officials rebutted—and policy makers were criticized for not being more attuned to the intelligence they were receiving. However, no one has been able to make the case that sufficient intelligence existed to forecast the time and place of the attacks. The admonition about strategic versus tactical surprise is apropos. (See chap. 1.) Stopping a terrorist attack requires tactical insights into the terrorists’ plans.

In the case of Iraq, the critique is just the opposite, that is, that intelligence analysts made too many unsubstantiated connections among various pieces of collected intelligence and created a false picture of the state of Iraq WMD programs. Implicit in this critique is the view, held by some, that analysts should not analyze beyond the collected intelligence lest they draw the wrong conclusions. This would be a deviating and alarming practice from the norm, given the likelihood at all times of less than perfect collection. Analysts are trained to use their experience and their instinct to fill in the collection gaps as best they can. That is one of the value-added aspects of analysts.

If a lesson is to be drawn from these two analytical experiences, it may be no more than that the analytical process is imperfect under any and all conditions. No Goldilocks formula has been devised as to the right amount of intelligence on which analysis should be based. The quality of that intelligence matters a great deal, as does the nature of the issue being analyzed.

The Office of the DNI addressed the sourcing issue in an intelligence community directive (ICD) in 2007. ICD 206 establishes sourcing and reference citation requirements for analytic products. This ICD was a response to some of the problems encountered in the Iraq WMD estimate, where judgments...
were not always clearly associated with the underlying intelligence, making it difficult for readers to determine the substantive basis for these judgments. Although intended as a guideline, ICD 206 is written in fairly adamant terms and allows for few exceptions. As a result, managers and analysts in several analytic offices have been unwilling to write analyses that could not be fully sourced and footnoted. This self-limitation was not the effect that the drafters of the ICD had in mind, but it does reflect some of the lingering after-effects of the Iraq NIE experience and attempts to solve perceived problems.

One of the distinctions that analysts like to make—and that also helps underscore the issue of dealing with limited information—is the difference between secrets and mysteries. Secrets are items of knowledge that are known to someone, just not to us. For example, there are Iranians who know the details and intent of their nuclear program. Mysteries are things that are not known and probably not knowable. For example, who built Stonehenge? Intelligence agencies exist to resolve secrets—either by penetrating them outright or by collecting against them and providing analysis. Mysteries fall into a different category. But there are times when the question being asked by the policy maker is more of a mystery than a secret. The analyst would like to beg off but often cannot.

Finally, there has been an increased emphasis, among policy makers and observers of the intelligence community, to ensure that analysts have access to and check all available data. This preference is an outgrowth of the failure among some agencies to share information prior to 9/11 and the “connect the dots” metaphor. After all, if one just connects all of the dots, then the answer should be there. (This is similar to the belief of big data advocates that the answer must lie somewhere in the data, if we just analyze enough of it.) As an example, in the aftermath of the failed Christmas 2009 airline bombing attempt in Detroit, President Obama excoriated the intelligence community for not sharing all of the available intelligence. In reality, few analysts will ever be sure that they have seen all of the available intelligence on a given issue unless it is relatively unimportant and therefore has little intelligence associated with it. But the emphasis on analysts seeing “everything” and checking all databases can lead to timidity on the part of analysts, who will become leery of publishing anything lest they are found to have missed some piece of intelligence. So, instead of learning to deal with limited information, one could end up with analysts who will not be willing to publish unless they are fairly certain that they have all of the information, largely to avoid being criticized should they miss something that leads to an unfortunate result.

Conveying Uncertainty. Just as everything may not be known, so, too, the likely outcome may not be clear. Conveying uncertainty can be difficult.
Analysts shy away from the simple but stark “We don’t know.” After all, they are being paid, in part, for making some intellectual leaps beyond what they do know. Too often, analysts rely on weasel words to convey uncertainty: “on the one hand,” “on the other hand,” “maybe,” “perhaps,” and so on. (President Harry S. Truman was famous for saying he wanted to meet a one-armed economist so that he would not have to hear “on the one hand, on the other hand” economic forecasting.) These words may convey analytical pusillanimity, not uncertainty. (Conveying uncertainty seems to be a particular problem in English, which is a Germanic language and makes less use of the subjunctive than do the Romance languages.)

Some years ago, a senior analytical manager crafted a system for suggesting potential outcomes by using both words and numbers—that is, a 1-in-10 chance, a 7-in-10 chance. Such numerical formulations may be more satisfying than words, but they run the risk of conveying to the policy client a degree of precision that does not exist. What is the difference between a 6-in-10 chance and a 7-in-10 chance, beyond greater conviction? It is also important to remember that an event that has a 6-in-10 chance of occurring also has a 4-in-10 chance of not occurring. When presented this way, the event now may seem uncomfortably close to 50/50, which a 6-in-10 chance does not convey by itself. There are very few “sure things.” In reality, the analyst is back to relying on gut feeling. (One chairman of the NIC became incensed when he read an analysis that assessed “a small but significant chance” of something happening.)

One way to help convey uncertainty is to identify in the analysis the issues about which there is uncertainty or the intelligence that is essentially missing but that would, in the analyst’s view, either resolve the unknowns or cause the analyst to reexamine currently held views. This raises another issue: known unknowns (that is, the things one knows that one does not know) versus the unknown unknowns (that is, the things one did not know that one did not know). By definition, the second group cannot be bounded or reduced as it is unknown. But one’s analysis must constantly be examined to identify known unknowns and to give attention to resolving these issues, if possible.

The use of language is important in all analysis. Analysts tend to use a stock set of verbs to convey their views: “believe,” “assess,” “judge.” For some analysts, the words have distinct and separate meanings that convey the amount of intelligence supporting a particular view and their certainty about this view. However, the intelligence community did not reach a consensus as to what each verb meant until 2005. The NIC now publishes an explanatory page with each NIE that explains the use of estimative language. The text box, “What We Mean When We Say: An Explanation of Estimative Language,” in the July 2007 NIE, The Terrorist Threat to the Homeland, is a useful example.
Terms like “we judge” or “we assess” are used interchangeably. (This seems close to the British experience on this issue, according to the 2004 British Butler report on intelligence about Iraq WMD. The Butler report states that British policy makers assumed the different words had different meanings, but British analysts said they just wrote naturally, using the terms interchangeably.) Analytical judgments can be based on collected intelligence or previous judgments that serve as “building blocks.” The use of “precise numerical ratings” is rejected as these “would imply more rigor than we intend.” Instead, there is a range of likelihood outcomes:

- Remote
- Unlikely
- Even chance
- Probably, likely
- Almost certainly

Note that there is no certainty at either end of this range. An event that is known to have no chance of occurring will not be analyzed. Nor will an event that is certain to occur be analyzed in terms of likelihood, although its ramifications can be discussed. Phrases like “we cannot rule out” or “we cannot discount” reflect an event that is seen as being unlikely or even remote but “whose consequences are such that it warrants mentioning.” These phrases are classic estimative language and can be interpreted by some readers, again, as a pusillanimous call. Finally, the use of “maybe” and “suggest” are defined as events the likelihood of which cannot be assessed because of a paucity of information.

Beyond these uses of language, there is the issue of the confidence that the analyst has in his or her judgments, called confidence levels. In NIEs, the confidence levels are “based on the scope and quality of information supporting our judgments.”

- High confidence: judgments based on high-quality information, or the nature of the issue makes a solid judgment possible
- Moderate confidence: available information is susceptible to multiple interpretations; or there may be alternative views; or the information is “credible and plausible” but not sufficiently corroborated
- Low confidence: information is scant, questionable, or fragmented, leading to difficulties in making “solid analytic inferences”; or is based on sources that may be problematic
Publishing a text box of this sort is a major step forward in trying to get the policy readers to understand the basis by which judgments are made. This also depends on policy makers reading it, and even this will not preclude future misunderstandings about the use of estimative language. Those who do read it will get a much better idea of the layers of meaning inherent in an estimative judgment. There are few, if any, straightforward calls.

A recent example of this issue of confidence levels came in 2013 when a DIA assessment of North Korea’s ability to reduce a nuclear weapon to a size that would fit on a missile was inadvertently disclosed during a congressional hearing. The DIA analysis had “moderate confidence” that North Korea had this capability. Some participants in the hearing dismissed the DIA analysis because it was “only” moderate confidence, apparently not understanding the full meaning of that phrase as defined above. These participants apparently believed that anything less than high confidence can be dismissed, which shows a misunderstanding of how intelligence analysis is written. DNI Clapper later testified that the DIA confidence was higher than the rest of the intelligence community but also noted that these types of disagreements are typical in a competitive analysis process.

**Indications and Warning.** Indications and warnings, or I&W, as it is known among intelligence professionals, is one of the most important roles of intelligence—giving policy makers advance warning of significant, usually military, events. The emphasis placed on I&W in the United States reflects the cold war legacy of a long-term military rivalry and the older roots of the U.S. intelligence community in Pearl Harbor, the classic I&W failure.

I&W is primarily a military intelligence function, with an emphasis on surprise attack. It relies, to a large extent, on the fact that all militaries operate according to certain regular schedules, forms, and behaviors, which provide a baseline against which to measure activity that may raise I&W concerns. In other words, analysts are looking for anything that is out of the ordinary, any new or unexpected activity that may presage an attack: calling up reserves, putting forces on a higher level of alert, dropping or increasing communications activity, imposing sudden communications silence, or sending more naval units to sea. But none of these can be viewed in isolation; they have to be seen within the wider context of overall behavior.

During the cold war, for example, U.S. and North Atlantic Treaty Organization (NATO) analysts worried about how much warning they would receive of a Warsaw Pact attack against Western Europe. Some analysts believed that they could provide policy makers, minimally, several days’ warning, as stocks were positioned, additional units were brought forward, and so on. Others believed that the Warsaw Pact had sufficient forces and
supplies in place to attack from a standing start. Fortunately, the issue was never put to the test.

For analysts, I&W can be a trap rather than an opportunity. Their main fear is failing to pick up on indicators and give adequate warning, which in part reflects the harsh view about intelligence when it misses an important event. In reaction, analysts may lower the threshold and issue warnings about everything, in effect crying wolf. Although this may reduce the analyst’s exposure to criticism, it has a lulling effect on the policy maker and can cheapen the function of I&W. A classic case of an I&W failure was Israeli I&W prior to the 1973 Yom Kippur War. Israeli military intelligence knew that the Egyptians would have to cross the Suez Canal to initiate war and established an elaborate I&W list. However, when the observed Egyptian activities did not conform to the established list, abetted by an Egyptian deception campaign, alarms were not raised, resulting in a surprise attack. In other words, the analysts became prisoners of their own I&W list.

Terrorism presents an entirely new and more difficult I&W problem. Terrorists do not operate from elaborate infrastructures, and they do not need to mobilize large numbers of people for their operations. One attraction of terrorism as a political tool is the ability to have a large effect with minimal forces. Thus, an entirely new I&W concept is needed to fight terrorism, one more likely to catch the much smaller signs of impending activity. In some respects, the I&W function for terrorism becomes very close to police work and keeping watch over neighborhoods or precincts, looking for things that “just don’t look right.” Terrorism also raises the duty-to-warn issue. If credible evidence indicates a potential attack, does the government have a responsibility to warn its citizens? A warning may tip off the terrorists to the fact that their plot has been penetrated, thus putting sources and methods at risk. Also, citizens may become inured to—if not downright cynical about—recurring changes in the level of warning, especially if the attacks do not occur. Some may come to believe that the government, and especially the intelligence agencies, is trying to cover itself in case an attack does occur. This phenomenon has been seen in the United States since 2001 as alerts have been issued and then withdrawn after the threat subsided or failed to materialize.

Opportunity Analysis. I&W is not only one of the most important analytic functions, but it is also one that comes naturally to intelligence analysts. A primary reason to have intelligence agencies is to avoid strategic surprise. (See chap. 1.) I&W is a means to that end. But I&W can become something of a trap, a theme that is reverted to too often lest something be missed.

Policy makers understand that I&W leaves them in the position of reacting to intelligence. But policy makers also want to be actors, to achieve goals and not
just prevent bad things from happening. As more than one senior policy maker has said, “I want intelligence that helps me advance my agenda, that makes me the actor, not the reactor.” This is often referred to as opportunity analysis.

Opportunity analysis is a sophisticated but difficult type of analysis to produce. First, it requires that the intelligence managers or analysts have a good sense of the goals that the policy maker seeks to achieve. Successful opportunity analysis may require some degree of specific and detailed knowledge of these goals. For example, knowing that a goal is arms control may not suggest many useful avenues of opportunity analysis beyond broad generalities. Knowing that the goals include certain types of weapons or restrictions would be more helpful. Thus, again, emphasis is placed on the importance of the intelligence analysts knowing the intended directions of policy. Second, opportunity analysis often seems more difficult or riskier as it requires positing how foreign leaders or nations will react to policy initiatives. Positing a foreign action and then describing either the consequences or possible reactions often seems easier than the reverse process. After all, an analyst often feels more comfortable understanding how a nation or its policy makers are likely to react even if the analyst is an expert in the politics of another country. Finally, opportunity analysis brings the intelligence community close to the line separating intelligence from policy. Writing good opportunity analysis without appearing to be prescriptive can be difficult even if that is not the intended message or goal.

In general, opportunity analysis is not engaged in often and is easily misunderstood when it is produced. However, opportunity analysis remains an important component of the National Intelligence Strategy.

An excellent example of opportunity analysis was the intelligence support that helped President George W. Bush decide to negotiate with Muammar Qaddafi about Libya’s covert WMD programs in 2003. The end result was the transfer of a variety of WMD components to the United States, which was not only important in its own right but seemed even more important in 2011 when NATO began an air campaign against Libyan forces trying to suppress a revolt, secure in the knowledge that Libya had little WMD at its disposal.

Alternative Analysis. One critique of the intelligence community’s performance on Iraq WMD was the alleged failure to examine alternative analytical lines. Even if true, it remains difficult in the case of Iraq to come up with analytically and intellectually sensible arguments that, in 2003, Saddam Hussein had come clean and had no WMD and was telling the truth when he made this case. Still, looking beyond the Iraq WMD case, the issue of alternative analysis is an important one. The 2004 intelligence law requires that the DNI create a process to ensure the effective use of alternative analysis.
The main driver is the concern that analysts can fasten on to one line of analysis, especially for issues that are examined and reexamined over the years, and then will not be open to other possible hypotheses or alternatives. (This behavior is called premature closure.) Should this happen, the analyst will then not be alert for changes, discontinuities, or surprises, even if they are not threatening. One way to attempt to avoid this potential intellectual trap is to create teams to draft alternative analyses, which are sometimes called red cells.

For several reasons, the intelligence community has not always embraced the concept. First, concerns arise that the process can be political in nature or can lead to politicization. The Team A and Team B example from the cold war (see chap. 11) remains a warning in this regard. The alternative analysis group (Team B) was made up of individuals who were more hawkish about dealing with the Soviet Union. Thus, it was no surprise that they found the NIEs on Soviet strategic goals wanting. The existence of an alternative analysis, especially on controversial issues, can lead policy makers to shop for the intelligence they want or cherry-pick analysis, which also results in politicization. Second, only so many analysts are available to deal with any issue or have the requisite expertise on any issue. Therefore, a decision has to be made as to which analysts are assigned to the mainstream and which to the alternative group. Their levels of expertise should be roughly equal. For analysts who have been on the losing side of issues in the area in the past, the chance to participate in alternative analysis may be an irresistible opportunity to reopen old arguments or settle scores. Finally, one of the prerequisites for alternative analysis is that it provides a fresh look at an issue. Therefore, as soon as this type of capacity is institutionalized and made a regular part of the process, it loses the originality and vitality that were sought in the first place.

Alternative analysis consists of more than simply asking a contrafactual question. As in the case of Iraq WMD, the contrafactual question (make the case that Saddam is telling the truth and has no WMD) would likely not have yielded a better analytical result. The analyst or the analytical manager has to be alert to the nature of the issue under consideration and the type of contrafactual question that will actually probe the generally held premise. It may be necessary to try several such questions before coming up with one that truly challenges the prevailing wisdom. In the case of Iraq WMD, a better question to ask might have been, What would Iraq look like if it did not possess WMD? Some analysts might have recognized that the Iraq they were analyzing could easily be viewed either way. This might not have changed the outcome of the NIE, as it still seemed more likely that Iraq did possess WMD, but at least the analysts would have probed alternatives.

The 2004 intelligence law puts great emphasis on alternative analysis, competitive analysis, and red teaming, which are all variants on the
same theme—an effort to avoid groupthink. The DNI is responsible for institutionalizing processes for these other types of analysis.

The intelligence community has long sought analytic tools, which means both programs and techniques that will foster better analysis. The computer industry has advanced the intelligence community’s ability to collect, manipulate, and correlate data, all of which eases part of the analyst’s burden. But there have also been problems integrating the tools into the analytic process, in large part because of the intellectual disconnect between those responsible for designing the tools and the analysts. Programmers and analysts do not think along similar lines, and too many programs have been developed without regard to how analysts think or work. Also, too few of the tools have been tested by working analysts. The net result has often been a new program that sits unused on an analyst’s computer desk top because it is either overly complex or not complementary to the analyst’s working methods.

There are also a variety of analytic techniques available to analysts. One of the more popular ones, in the aftermath of 9/11 and Iraq, is alternative competing hypotheses (ACH). ACH offers a simple way to ensure that multiple plausible explanations for the known intelligence are considered, as well as assessing which hypotheses are more likely by building a matrix to consider alternative scenarios. The Defense Intelligence Agency (DIA) is now experimenting with “object-based production” (OBP)—that is, organizing available data from all INTs on the “object” of concern, meaning an issue or actor. The belief is that by organizing the intelligence in this way, the “knowns” will be more readily identified, as will, presumably, the unknowns. DIA also believes that OBP can be enhanced by applying some of the techniques and lessons learned in activity-based intelligence (ABI) in collection (see chap. 5), which will help associate discovered activities with “objects.”

Various techniques have strong advocates both inside and beyond the intelligence community. But it is best to think about these like tools, no different than a homeowner’s toolbox. No tool is right for every job. They key is to be conversant with the tools and to know which one is right for which analytical job.

**Estimates.** The United States creates and uses analytical products called estimates (or assessments in Britain and Australia). These serve two major purposes: to see where a major issue or trend will go over the next several years and to present the considered view of the entire intelligence community, not just one agency. In the United States, the NIE’s community-wide basis is signified by the fact that the DNI signs completed estimates, just as DCIs did before.
Estimates are not predictions of the future but rather considered judgments as to the likely course of events regarding an issue of importance to the nation. Often, more than one possible outcome may be included in a single estimate. The difference between estimate and prediction is crucial but often misunderstood, especially by policy makers. Prediction foretells the future—or attempts to. Estimates are vaguer, assessing the relative likelihood of one or more outcomes. If an event or outcome were predictable—that is, capable of being foretold—one would not need intelligence agencies to estimate its likelihood. It is the uncertainty or unknowability that is key. To quote Yogi Berra again, “It is very difficult to make predictions, especially about the future.”

The bureaucratics of estimates are important to their outcome. In the United States, national intelligence officers are responsible for preparing estimates. They circulate the terms of reference (TOR) among colleagues and other agencies at the outset of an estimate. The TOR may be the subject of prolonged discussion and negotiation, as various agencies may believe that the basic questions or lines of analysis are not being framed properly. Shaping the TOR is crucial to the outcome of the estimate. Drafting is not done by the NIOs but by someone from the NIO’s office, or the NIO may recruit a drafter from one of the intelligence agencies. Once drafted, the estimate is coordinated with other agencies, that is, the other agencies read it and give comments, not all of which are accepted, because they may be at variance with the drafter’s views. Numerous “coordination” meetings are held to resolve disputes, but the meetings may end with two or more views on some aspects that cannot be reconciled. The DNI chairs a final meeting, a National Intelligence Board, which is attended by senior officials from a number of agencies. After the DNI signs the estimate, signifying he or she is satisfied with it, the DNI owns the estimate. DCIs were known to change the views expressed in estimates with which they disagreed. This usually displeased the drafter but was within the DCI’s authority.

In addition to the bureaucratic game playing that may be involved in drafting estimates, issues of process influence outcomes. Not every issue is of interest to every intelligence agency. But each agency understands the necessity of taking part in the estimative process, not only for its intrinsic intelligence value but also as a means of keeping watch on the other agencies. Furthermore, not every intelligence agency brings the same level of expertise to an issue. For example, the State Department is much more concerned on a day-to-day basis about human rights violations than are other agencies, and INR reflects this in its work for its specific policy makers and in the expertise it chooses to develop on this issue. Or, the Department of Defense (DOD) is much more concerned about the infrastructure of a nation in which U.S. troops may be deployed.
Rightly or wrongly, however, estimates are egalitarian experiences in that the views of all agencies are treated as having equal weight. This ignores the Orwellian view of intelligence that holds, on certain issues, that some agencies are “more equal” than others.

Some issues are the subjects of repeated estimates. For example, during the cold war, the intelligence community produced an annual estimate (in three volumes) on Soviet strategic forces, NIE 11–3-8. For issues of long-term importance, regular estimates are a useful way of keeping track of an issue, of watching it closely and looking for changes in perceived patterns. However, a regularly produced estimate can also be an intellectual trap, as it establishes several benchmarks that analysts do not want to tinker with in the event of possible changes. Having produced a long-standing record on certain key issues, the estimative community finds it difficult to admit that major changes are under way that, in effect, undercut its past analysis.

This issue may be less crass than preserving one’s past record. Having come to a set of conclusions based on collection and analysis, what does it take for an analyst or a team of analysts working on an estimate to feel compelled to walk away from their past work and come to an opposite conclusion? One can create a scenario in which some new piece of intelligence completely reverses analysts’ thinking. Such an occasion is extremely rare. Is it possible to start from scratch and ignore past work? If one tries to, what is the cutoff point for old collection that is no longer of use? Although the influence of past analysis can be a problem, it is less easily solved than is commonly thought. Intelligence analysis is an iterative process that lacks clear beginning and end points for either collection or analysis. The case of the 2007 Iran nuclear estimate is again instructive. According to intelligence officials, newly available intelligence only came to light very late in the estimative process. The implications of the new intelligence were clear and stark. The first issue to be dealt with was the veracity of the new intelligence: Was it being fed by Iran? Although this question cannot be answered definitively, analysts who subjected the new intelligence to rigorous examination came away convinced that it was real. This meant that the conclusions of the estimate had to be revised, with all of the attendant reaction discussed earlier. Although those responsible for the Iran nuclear NIE stand by their analysis, they also admit that it is not a certainty and will remain subject to change.

Some people question the utility of estimates. Both producers and consumers have had concerns about the length of estimates and their sometimes plodding style. Critics also have voiced concerns about timeliness, in that some estimates take more than a year to complete. One of the worst examples of poor timing came in 1979. An estimate on the future political stability of Iran was being written—including the observation that Iran was
“not in a prerevolutionary state”—even as the shah’s regime was unraveling daily. This incongruity led the House Intelligence Committee to observe that estimates “are not worth fighting over.” In 2010, the NIC made a series of changes to the structure of NIEs to respond to some of these criticisms. Among these are limiting the main body text to twenty pages (down from an average length of fifty-four to sixty-eight pages); limiting Key Judgments (KJs) to two to three pages; and tightening the linkages between the KJs and the supporting analysis.

After the start of the Iraq war (2003–2011), the estimate process came under intense scrutiny and criticism, prompted by the Iraq WMD NIE. Among the concerns were the influence of past estimates, the groupthink issue, the use of language that seemed to suggest more certainty than existed in the sources, inconsistencies between summary paragraphs (KJs) and actual text, and the speed with which the estimate was written. This last criticism was interesting in that the estimate was written at the request of the Senate, to meet its three-week deadline before voting on the resolution granting the president authority to use force against Iraq. Frequent leaks of NIEs on a variety of Iraq-related topics led some to charge that the intelligence community was at war with the Bush administration.

After the Iraq WMD NIE, there was increased political pressure, largely coming from Congress, to have at least the KJs of the estimates made public. The KJs for Prospects for Iraq’s Stability: A Challenging Road Ahead (January 2007) and The Terrorist Threat to the Homeland (July 2007) were published. As could be expected, members of Congress who took issue with the Bush administration’s policies used these published documents as confirmation of their own political stances. Although this does not contravene any rules or procedures, it does have the effect of immediately injecting the NIEs into a partisan debate. On October 24, 2007, DNI McConnell announced his judgment that declassified KJs should not be published and that he did not accept the recent publication as a precedent. However, the Iran nuclear NIE’s KJs were published just seven weeks later, undercutting McConnell’s stance. This practice actually ended after the Iran NIE. There are many costs in publishing NIEs, in whole or in part. It can affect the willingness of analysts or NIE managers to make strong calls because of their reluctance to be drawn into partisan debates. It also tends to misuse NIEs as factual refutations of administration policies, thus changing the very basis by which an estimate is crafted. Also, given the instant political analysis to which released NIEs are subject, this process has the odd effect of taking a strategic document and turning it into current intelligence.

In addition to being made shorter (twenty pages maximum) the NIC has made other changes to improve the rigor of NIEs. Judgments are now
accompanied by assessments of likelihood or probability and confidence statements. NIEs also include risks and opportunities analysis, and they identify collection gaps or alternative scenarios.

It is also possible that too much emphasis has been put on estimates. Although they do represent the collective views of the intelligence agencies and are signed by the DNI and given to the president, estimates are not the only form of strategic intelligence produced within the analytic community. However, estimates—or the lack of them—have come to be seen, incorrectly, as the only indicator of whether the intelligence community is treating an issue strategically. This certainly was the critique of the 9/11 Commission, whose report castigated the community for not producing an NIE on terrorism for several years before 9/11. Strategic intelligence analysis can take many forms and can be written either by several agencies or by one. NIEs are not the only available format, and their existence or absence does not indicate the seriousness with which the intelligence community views an issue.

**Competitive Analysis.** The U.S. intelligence community believes in the concept of competitive analysis—having different agencies with different points of view work on the same issue. Because the United States has several intelligence agencies—including three major all-source analytical agencies (CIA, DIA, and INR)—every relevant actor understands that the agencies have different analytical strengths and, likely, different points of view on a given issue. By having each of them—and other agencies as well on some issues—analyze an issue, the belief is that the analysis will be stronger and more likely to give policy makers accurate intelligence.

Beyond the day-to-day competition that takes place among the intelligence publications of each agency, the intelligence community fosters competition in other ways. Intelligence agencies occasionally form red teams, which take on the role of the analysts of another nation or group as a means of gaining insights into their thinking. A now-famous competitive exercise was the already noted 1976 formation of Teams A and B to review intelligence on Soviet strategic forces and doctrine. Team A consisted of intelligence community analysts, and Team B consisted of outside experts, but with a decidedly hawkish viewpoint. The teams disagreed little on the strategic systems the Soviets had built; the key issue was Soviet nuclear doctrine and strategic intentions. Predictably, Team B believed that the intelligence supported a more threatening view of Soviet intentions. However, the lack of balance on Team B largely vitiated the exercise, which could have been useful not only for gaining insight into Soviet intentions but also for validating the utility of competitive intelligence exercises.

Dissent channels—bureaucratic mechanisms by which analysts can challenge the views of their superiors without risk to their careers—are helpful
but not widely used. Such channels have long existed for Foreign Service
officers in the State Department. Although less effective than competitive
analysis for articulating alternative viewpoints, they offer a means by which
alternative views can survive a bureaucratic process that tends to emphasize
mutual consent.

A broader issue is the extent to which competitive intelligence can or
should be institutionalized. To some degree, in the U.S. system it already is.
But the competition among the three all-source agencies is not always pointed.
They frequently work on the same issue, but with different perspectives that
are well understood, thus muting some of the differences that may be seen.

Competitive analysis requires that enough analysts with similar areas of
expertise are working in more than one agency. This was certainly true during
the zenith of competitive analysis, in the 1980s. But the capability began to
dwindle as the intelligence community faced severe budget cuts and personnel
losses in the 1990s, after the end of the cold war. As analytic staffs got smaller,
agencies began to concentrate more on those issues of greatest importance
to their policy customers. Thus, the ability to conduct competitive analysis
declined. To rebuild the capability requires two things: more analysts and the
time for them to become expert in one or more areas. As the intelligence budgets
decline—which is likely to continue regardless of the fate of sequestration—
preserving this competitive analytic capability will once again be an issue.

Although the intelligence community believes in competitive analysis, not
all policy makers are receptive to the idea. Some see no reason why agencies
cannot agree on issues, perhaps assuming that each issue has a single answer
that should be knowable. One main reason that President Truman created the
Central Intelligence Group (CIG) and its successor, the CIA, was his annoyance
over receiving intelligence reports that did not agree. He wanted an agency to
coordinate the reports so that he could work his way through the contradictory
views. Truman was smart enough to realize that agencies might not agree, but
he was not comfortable receiving disparate reports without some coordination
that attempted to make sense of the areas of agreement and disagreement.
Other policy makers lack Truman’s subtlety and cannot abide having agencies
disagree, thus vitiating the concept of competitive analysis.

Finally, those who are not familiar with the idea of competitive analysis,
and even some who are, may regard the planned redundancy as more wasteful
than intellectually productive.

**Multi-Int Versus All-Source Analysis.** As noted in chapter 5, there has
been growing tension and some confusion about the differences between
and the relative benefits of multi-intelligence (usually called multi-int) and
all-source intelligence. To repeat, multi-int is a combining of two or more
technical intelligence sources, most often geospatial intelligence (GEOINT) and signals intelligence (SIGINT). Again, multi-int is more than a single INT but less than all-source. To be clear, this is not an all-or-nothing issue. There are times when a multi-int analysis may be the sufficient, if not proper, response and times when all-source is required. However, some problems have arisen, at least in the view of those responsible for all-source. One concern is that the policy maker, who is less facile with these intelligence nuances, may be reading a multi-int product and not realize that it is not all-source. This may or may not affect the value of the analysis, but for a policy maker, the ability to make that judgment is difficult as he or she will not readily understand the difference and what may be missing in a multi-int analysis that might have been available in all-source. Second, there is a concern that the analysts who contribute to multi-int analyses are, in essence, single INT analysts and do not have the same analytic depth that an all-source analyst is expected to have. There have been instances in which multi-int analyses have gotten beyond their depth, especially when they venture into political analyses. At the same time, the managers of the analysts writing multi-int are pleased to be bridging the stovepipes and sometimes take umbrage when it is suggested that their analysts have some limitations.

There is a need for both types of analysis, but some “rules of the road” about who does what would probably improve the products, as would some labeling so that policy makers know at the outset the basis of the analysis they are reading.

**Politicized Intelligence.** The issue of politicized intelligence arises from the line separating policy and intelligence. This line is best thought of as a semipermeable membrane; policy makers are free to offer assessments that run counter to intelligence analyses, but intelligence officers are not allowed to make policy recommendations based on their intelligence. For example, in the State Department in the late 1980s, the assistant secretary responsible for the Western Hemisphere, Elliot Abrams, often disagreed with pessimistic INR assessments as to the likelihood that the contras would be victorious in Nicaragua. Abrams would often write more positive assessments on his own that he would forward to Secretary of State George P. Shultz.

Policy makers and intelligence officers have different institutional and personal investments in the issues on which they work. The policy makers are creating policy and hope to accrue other benefits (career advancement, reélection) from a successful policy. Intelligence officers are not responsible for creating policy or for its success, yet they understand that the outcomes may affect their own status, both institutional and personal.
The issue of politicization arises primarily from concerns that intelligence officers may intentionally alter intelligence, which is supposed to be objective, to support the options or outcomes preferred by policy makers. These actions may stem from a number of motives: a loss of objectivity regarding the issue at hand, a preference for specific options or outcomes, an effort to be more supportive, career interests, or outright pandering.

Intentionally altering intelligence is a subtle issue because it does not involve crossing the line from analysis to policy.

Instead, the analyst is tampering with his or her own product so that it is received more favorably. The issue is also made more complex by the fact that at the most senior levels of the intelligence community, the line separating intelligence from policy begins to blur. Policy makers ask senior intelligence officials for their personal views on an issue or policy, which they may give. It is difficult to conceive of a DNI or a DCI always abstaining when the president or the secretary of state asks such a question.

The size or persistence of the politicization problem is difficult to determine. Some who raise accusations about politicized intelligence are losers in the bureaucratic battles—intelligence officers whose views have not prevailed or policy makers (in the executive branch or Congress, either loyal to the current administration or in opposition) who are dissatisfied with current policy directions. Thus, their accusations may be no more objective than the intelligence that concerns them. Those unfamiliar with the process are often surprised to hear intelligence practitioners talk about winners and losers. But these debates—within the policy or the intelligence community—are not abstract academic discussions. Their outcomes have real results that can be significant and even dangerous. Analysts’ careers can rise and fall as well as a result of which side of a debate they are on. Just as intelligence officers serve policy makers, career officers—both intelligence and policy—serve political appointees, who are less interested in the objectivity of analysis.

For example, in the late 1940s and early 1950s, many State Department experts on China (the “China hands”) had their careers sidetracked or were forced from office over allegations that they had “lost” China to the communists. Numerous scholars and officials interpreted their treatment as a gross injustice. But, as Harvard University professor Ernest R. May pointed out, the U.S. public in the elections of the early 1950s largely repudiated the anti-Chiang Kai-shek views of the China hands by returning the pro-Chiang Republicans to power. So the China hands not only had ideological foes within the government, but they also had no political basis on which to pursue their preferred policies. Similarly, the careers of many intelligence officers and Foreign Service officers involved in crafting and promoting the strategic arms limitation talks (SALT II) treaty during the Carter administration failed
Intelligence: From Secrets to Policy
to prosper when Ronald Reagan, who opposed the treaty, took office. Again, their careers suffered only because of an electoral victory. One can argue that these punishments were not what the electorate had in mind, but they underscore the fact that the government and the underlying policy processes are essentially political in nature.

Politicization by intelligence officers may also be a question of perception. A consensus could probably be reached on what politicized intelligence looked like, but much less agreement would emerge on whether a specific analysis fit the definition.

Thus, politicized intelligence remains a concern, albeit a somewhat vague one, which may make it more difficult and important. Many issues surrounding politicized intelligence came up in the hearings on Robert Gates’s second nomination as DCI, when several analysts charged that Gates had altered analyses on the Soviet Union to meet policy makers’ preferences. Gates asked President Reagan to withdraw his first nomination in 1986, during the Iran-contra affair. He was subsequently renominated by President George H. W. Bush and confirmed in 1991.

Politicization was also a concern in the Iraq WMD issue. In 2003, the press reported that Vice President Dick Cheney had been out to the CIA several times to receive briefings on Iraq. Critics saw the visits as an attempt to influence the analysts, even though intelligence officials and analysts maintained that they were not asked to alter their analyses. Is there a proper number of times a senior official should be briefed on a highly sensitive topic, after which it appears to be politicization? The answer likely is no. What matters is the substance of the exchange. Also, such exchanges are a primary reason for intelligence agencies—to help officials make decisions. In Britain, charges of politicization on Iraq centered on accusations that Prime Minister Tony Blair or his office asked Defence Ministry officials to “sex up” their intelligence on Iraq WMD, which the government denied. Three external reviews of intelligence on Iraq, by the Senate Intelligence Committee and the WMD Commission in the United States and by Lord Butler in Britain, all concluded that the intelligence had not been politicized. A fourth report, done for the Australian government, came to the same conclusion.

A second type of politicized intelligence is caused by policy makers who may react strongly to intelligence, depending on whether it confirms or refutes their preferences for policy outcomes. For example, according to press accounts in November 1998, Vice President Al Gore’s staff rejected CIA reports about the personal corruption of Russian premier Viktor Chernomyrdin. Staff members argued that the administration had to deal with Chernomyrdin, corrupt or not, and that the intelligence was inconclusive. Analysts countered that the administration set the standard for proof so high that it was unlikely
to be met by intelligence. The analysts found that they were censoring their reports to avoid further disputes with the White House. Both policy and intelligence officers denied the allegations.

Policy makers may also use intelligence issues for partisan purposes. Two examples in the United States were the missile gap (1959–1961) and the window of vulnerability (1979–1981). In both cases, the party that was out of power (the Democrats in the first case, the Republicans in the second) argued that the Soviet Union had gained a strategic nuclear advantage over the United States, which was being ignored or not reported. In both cases, the accusing party won the election (not because of its charges) and subsequently learned that the intelligence did not support the accusations—which it then simply claimed had been resolved.

Analytical Standards. As this chapter has argued, there is a set of standards in intelligence analysis. Most of them are fairly well-known and accepted, although, until recently, little effort was made to codify them. This changed in the aftermath of the 2001 terrorist attacks and the Iraq WMD issue. The Intelligence Reform and Terrorism Prevention Act (IRTPA, 2004) includes a number of standards for intelligence analysis. The DNI’s office has also issued standards for evaluating intelligence.

It is important to understand analytic standards for their own sake, but they cannot be wholly separated from the circumstances in which they are written. The twin events of 9/11 and Iraq WMD left most observers with the overwhelming impression that the analytical capacity of the intelligence community was flawed and performed badly. However, as has been noted earlier, the perceived “lessons” of the two events tend to run in opposite directions.

- Warning: The “lesson” of 9/11 was that the intelligence community failed to be strident enough in its warnings, leaving policy makers with an imprecise sense of the impending nature of the threat. Intelligence officers serving at the time deny this and also note that the tactical intelligence that would have been useful did not exist. In the case of Iraq WMD, the intelligence community is said to have overblown the threat based on very little new intelligence.
- Analytical process: In 9/11, analysts failed to make the necessary linkages between disparate pieces of intelligence (hence, the “connect the dots” metaphor), but for Iraq WMD they made too many linkages, resulting in a false image of the WMD programs. The analysis before 9/11 has also been attacked as a “failure of imagination,” but in the case of Iraq, the analysis was seen as being perhaps too imaginative.
Information sharing: The failure to discover the 9/11 plot is ascribed, in part, to the failure of the CIA and the Federal Bureau of Investigation (FBI) to share information. But in the case of Iraq WMD, the intelligence community was taken to task for sharing information (the unreliable human source called CURVE BALL) that was not true, although those sharing it did not know that.

Therefore, when crafting the legislation creating the DNI, Congress went into unusual detail about what it expected of future analysis. The DNI must appoint an individual or office responsible for ensuring that finished intelligence produced by any intelligence community element is “timely, objective, independent of political considerations, based upon all sources of available intelligence, and employ the standards of proper analytic trade-craft” (Section 1019). This individual or office can have no direct responsibility for the specific production of any finished intelligence and must prepare regular detailed reviews of analytic products, lessons learned, and recommendations for improvement. The criteria for these evaluations and reviews are detailed. Finally, the act calls for the creation of what has become an analytic ombudsman. (See box, “How Right How Often.”)

The analytic overseers in the office of the DNI also created a set of evaluation tradecraft standards for analysis, few of which are controversial. They deal mostly with the underlying aspects of intelligence: sources, assumptions, judgments, alternative analyses, logical argumentation, and so on. The final standard, accuracy, may not be known for some time.

Most observers would likely agree that these are among the necessary standards for good analysis. The real concern is how these standards are put into practice. It is noteworthy that the standards reflect more of the perceived lessons of Iraq WMD than of September 11. The DNI’s office has stated that these standards will serve as community-wide guidelines, making them part of the training for all new analysts and for analytical managers. Given the paucity of community-wide courses, this training can capture only a small number of the analysts across the community in any given year and far fewer than the large numbers that have been recruited. Therefore, overseeing standards implementation requires insights into the analytic training being conducted at each agency. But, as noted regarding ICD 206 on sourcing, these standards also run the risk of being misinterpreted or having unintended consequences.

The use of these standards as an evaluation tool is more problematic. The congressional mandate for a broad review of finished intelligence products is impractical given the volume of intelligence produced daily. The most that can then be done is to sample, either by topic or by office, or both, and hope that some larger lessons can be drawn. This may prove difficult given the problems inherent in any sampling methodology.
The underlying question is the expectations of either Congress or the DNI’s office about how these standards might affect future analysis. It is possible, for example, to perform highly in each of the standards and still find, after the fact, that the judgments and assessments proved to be inaccurate. Value is given to consistency, which can run counter to the desire for analytic insight and the avoidance of groupthink. If the highest standard for analysis is accuracy, then we face the problem that neither these standards nor any others will guarantee that outcome. Clearly, these standards are more likely to result in analytic products that are sound in terms of methodology, but this is not the same as accuracy. Also, these standards run the risk of creating a very mechanistic approach to what is, at its core, an intellectual process. For example, the truly gifted and occasionally insightful analyst could get poor grades in most of these criteria and still produce an accurate and useful analysis.

**How Right How Often**

**The Nature of the Question: A Baseball Analogy**

One of the most persistent and unanswerable questions in intelligence analysis is this: How right should the analysts be how often? The answer depends, in part, on the available intelligence and the skills of the analyst. But there are also significant differences depending on the nature of the question being asked.

To use baseball as an analogy, there are only two activities happening in a ball game: fielding and hitting. But the standards for these two are very different. Professional baseball fielders are expected to perform in the range of .950, or better, out of a thousand. But across the major leagues, the batting average is around .260. So, clearly, batting is more difficult than fielding.

In terms of analysis, sometimes there are fielding questions. For example: Who is the commander of the North Korean air force, and what do we know about him? But sometimes there are batting questions: What is Kim Jung Un going to do next?

Therefore, analytic performance is also driven by the nature of the question being asked.

**The Analytic Workforce.** The demographics of the analysts in U.S. intelligence are driven first by the contraction that the intelligence community endured during the 1990s, suffering deep budget cuts after the cold war. The so-called cold war peace dividend fell more heavily in proportional terms on
intelligence than it did on defense. As DCI Tenet expressed it, the net result was the loss of 23,000 employees and positions across U.S. intelligence, meaning both people who left and—more significantly—people who were never hired. The second factor came in the aftermath of the 2001 terrorist attacks when all agencies began major hiring efforts. The result of these efforts has been a workforce of decreasing experience over time as new hires outnumber veterans, who continue to retire. In 2013, perhaps half of the analysts across the intelligence community had six years or less experience in their subject areas, leading some to observe that this is the least experienced analytic cadre since the formation of the intelligence community in 1947.

These demographic trends have several important implications for analysis:

- **Experience**: The most obvious issue is the relative inexperience of the workforce as analysts and subject matter experts. As discussed earlier, human intelligence (HUMINT) collectors need five to seven years to be considered seasoned. There is no agreed benchmark for analysts, but the five-year mark is probably a reliable one, give or take a year. This is sometimes referred to as the “green/gray” problem—that is, the analytic workforce is getting younger, not older. This is both a problem in and of itself and also a problem in terms of management. The cadre that should be moving into senior analytic management ranks is too thin to fill all of the necessary positions. This necessitates promoting more junior analysts sooner. Again, their lack of experience might become problematic.

- **Work methods**: The new cadre of analysts are more comfortable working in networks and working more collaboratively, both of which are positive attributes. They also are much more comfortable with information technology and working in a “softcopy” world. It is too soon to know, however, if they will be comfortable asserting themselves and their views when necessary or if they will default to lowest common denominator analyses as part of their collaborative instinct. It is also not clear how the new cadre of analysts will assess incoming intelligence. One of the charms of the World Wide Web is that it is a democratic institution: Anyone is free to post any of their views on any subject. This is also, from an intelligence viewpoint, a problem, as intelligence must address the issue of validity of sources: Who are they? What is their basis for saying this? Are they knowledgeable and credible? Do they have motives for saying this? If one thinks of the Web as a giant bulletin board where anything can be posted and shared, the ability to rise above that in working on intelligence becomes more evident. The Web may be an interesting metaphor for collaboration, but it can
be dangerous when assessing views and information. Moreover, for a
generation that uses social media as a major form of communication,
will they bring enough critical faculties to bear when assessing
intelligence derived from social media?

- Retention: A key issue for intelligence agencies is retaining as many of
these new analysts, or at least the good ones, as possible. Poor retention
rates will only replicate the current demographic problems that led to
this issue. Retention goes to the issues of career management, career
progression, and education and training. These have not been areas
to which managers have given much attention until recently, but they
will underpin much of the other efforts at transformation. There is
a budgetary aspect to this that will also affect the experience levels,
noted above. As the Afghan war winds down, the Defense budget will
lose a great deal of funding predicated on the Iraq and Afghan wars.
This funding helped support literally hundreds of contractors who
served as analysts at the various commands. Their contracts will not
be renewed, thus hurting the experience levels once again and creating
a “brain drain” as many of these analysts have more experience than
their intelligence community colleagues.

A final workforce issue results from the long war against terrorists,
buttressed to some degree by the campaigns in Iraq and Afghanistan. Although
there has been strategy guiding all three of these efforts, for the analysts
these have been largely tactical engagements, looking for small groups if not
individuals. Thus, many of the analysts who joined in the surge after 2001
have spent a good deal of their career on these tactical types of issues. The
effect has probably been most telling in the CIA. Former DCIA Michael
Current DCIA John Brennan (2013–) has spoken of the need to “demilitarize”
the CIA, in part for operational rather than analytical reasons.

At DIA, there has been some of the same effect, although it is less
pronounced there as DIA more often works on tactical issues in support
of fighting forces. However, in the workforce transition noted above there
has been a loss of analysts who had the substantive knowledge to help plan
conventional military campaigns, which has not been passed on to those who
followed and who have focused mostly on terrorism. But DIA faces another
conundrum, framed by this question: Are we doing defense intelligence or
intelligence for defense? What DIA managers and analysts mean when they ask
this question is that their preference is to do “defense intelligence”—that is, a
focus on defense-related intelligence issues. However, they are often required
to become the more general intelligence support, especially for the COCOMs,
on a host of political and economic issues because there is no one else in the intelligence community who will respond to these requests. Some DIA analysts believe these types of questions should more properly be answered by CIA, but CIA does not automatically respond to answer COCOM requests the way that DIA does. Both workforces, CIA and especially DIA, have also been stretched by the need to deploy analysts forward for long periods of time.

The problem now facing the intelligence community is how to begin transitioning some analysts away from terrorism and back to more traditional political–military issues that are strategic, rather than tactical, in nature. A major driver here is the Obama administration’s stated “rebalance” toward the Pacific. Many veteran analysts agree that it is more difficult to go from tactical issues to strategic issues than the other way around—but that is the task that now must be addressed.

This transition may be made more difficult if retention rates continue to decline, as they have done in recent years. For several years, intelligence managers were fairly callous about the retention issue, arguing that the recession made leaving government service very unattractive. However, as the economy has begun to improve, there are more noticeable losses of personnel to the private sector, which again affects experience levels but without necessary budget authority to fill vacated positions. The retention issue is also seen as a reflection of some poor management practices in some of the agencies. It may also reflect the burnout caused by working on relentlessly intense issues such as terrorism or supporting forces in active combat.

Intelligence Analysis: An Assessment

Sherman Kent, an intellectual founder of the U.S. intelligence community, especially of its estimative process, once wrote that every intelligence analyst has three wishes: to know everything, to be believed, and to influence policy for the good (as the analyst understands it). Kent’s three wishes offer a yardstick by which to measure analysis. Clearly, an analyst can never know everything in a given field. If everything were known, the need for intelligence would not exist—nothing would be left to discover. But what Kent is getting at is the desire of the analyst to know as much as possible about a given issue before being asked to write about it. The amount of intelligence available varies from issue to issue and from time to time. Analysts must therefore be trained to develop some inner, deeper knowledge that enables them to read between the lines, to make educated guesses or intuitive choices when the intelligence is insufficient.
Kent’s second wish—to be believed—goes to the heart of the relationship between intelligence and policy. Policy makers pay no price for ignoring intelligence, barring highly infrequent strategic disasters such as Josef Stalin’s refusal to accept the signs of an imminent German attack in 1941. Intelligence officers see themselves as honest and objective messengers who add value to the process, who provide not just sources but also analysis. Their reward, at the end of the process, is to be listened to, which varies greatly from one policy maker to another.

Finally, and derived from his second wish, Kent notes that intelligence officers want to have a positive effect on policy, to help avert disaster and to help produce positive outcomes in the nation’s interests. But analysts want to be more than a Cassandra, constantly warning of doom and disaster. Their wish to have a positive influence also indicates the desire to be kept informed about what policy makers are doing to enable the intelligence officers to play a meaningful role.

What, then, constitutes good intelligence? This is no small question, and one is reminded of Justice Potter Stewart’s opinion in a court case involving obscenity and pornography: “[I can’t define it,] but I know it when I see it.” Good intelligence has something of the same indistinct quality. At least four qualities come to mind. Good intelligence is:

- **Timely:** Getting the intelligence to the policy maker on time is more important than waiting for every last shred of collection to come in or for the paper to be pristine, clean, and in the right format. The timeliness criterion runs counter to the first of Kent’s three wishes: to know everything. Time can change the perspective on an occurrence. Napoleon died on St. Helena in May 1821; word of his death did not reach Paris until July. Charles Maurice de Talleyrand, once Napoleon’s foreign minister and later one of his foes, was dining at a friend’s house when they heard of Napoleon’s passing. The hostess exclaimed, “What an event!” Talleyrand corrected her: “It is no longer an event, Madam, it is news.”

- **Tailored:** Good intelligence focuses on the specific information needs of the policy maker, to whatever depth and breadth are required, but without extraneous material. This must be done in a way that does not result in losing objectivity or politicizing the intelligence. Tailored intelligence products (those responding to a specific need or request) are among the most highly prized by policy makers.

- **Digestible:** Good intelligence has to be in a form and of a length that allow policy makers to grasp what they need to know as easily as possible. The requirement tends to argue in favor of shorter intelligence products, but it is primarily meant to stress that the message be...
presented clearly so that it can be readily understood. This does not mean that the message cannot be complex or even incomplete. But whatever the main message is, the policy maker must be able to understand it with a minimum of effort. Being succinct and clear is an important skill for analysts to learn. Writing a good two-page memo is much more difficult than writing a five-page memo on the same subject. As Mark Twain observed in a letter to a friend, “I am writing you a long letter because I don’t have time to write a short one.”

- Clear regarding the known and the unknown: Good intelligence must convey to the reader what is known, what is unknown, and what has been filled in by analysis, as well as the degree of confidence in the material. The degree of confidence is important because the policy maker must have some sense of the relative firmness of the intelligence. All intelligence involves risk by the very nature of the information being dealt with. The risk should not be assumed by the analysts alone but should be shared with their clients.

Objectivity was not one of the major factors defining good intelligence. Its omission was not an oversight. The need for objectivity is so great and so pervasive that it should be taken as a given. If the intelligence is not objective, then none of the other attributes—timeliness, digestibility, clarity—matters.

Accuracy also is not a criterion. Accuracy is a more difficult standard for assessing intelligence than might be imagined. Clearly, no one wants to be wrong, but everyone recognizes the impossibility of infallibility. Given these limits, what accuracy standard should be used? One hundred percent is too high and 0 percent is too low. Splitting the difference at 50 percent accuracy is still unsatisfactory. Thus, what is left is a numbers game—something more than 50 percent and less than 100 percent. Accuracy can also be difficult to assess as many issues do not have definitive endings. Here we are back to the current versus long-term problem. Short-term issues are more likely to have specific endings (elections; specific decisions or actions); longer term issues will not. Therefore, it becomes more difficult to assess accuracy. For example, during the cold war, the United States maintained its policy of containment for more than forty years, despite the fact that there were not many signs of its being successful. Then, quite suddenly, between roughly 1989 and 1991, it worked. So, how would one have phrased assessments of containment over that period?

The issue of accuracy became more demanding in the aftermath of September 11 and the onset of the Iraq war. The political system seemed to have decreasing tolerance for the imperfection that is inherent in intelligence analysis. Even though all observers understand that perfection is not
possible, each and every mistake seemed to incur a large political cost for the intelligence agencies. This can have an additional cost in the analytic system if analysts become risk-averse because of the political costs of being wrong. Even though most observers would agree that 100 percent accuracy is unachievable, they would also argue that the “big things” are the issues where accuracy matters. Examples of such “big things” would be the existence of Iraq WMD or the impending fall of the Soviet Union. But these are the very issues where intelligence is more likely to be wrong because they run counter to years of collected intelligence and presumably accurate analyses. Recall the pearl metaphor discussed under collection: the slow, steady accumulation of intelligence over time, often decades. This accumulative process has an effect on the analysts. It leads them to create what they believe are accurate pictures of behavior and more or less likely outcomes. But the “big things” tend to be hardest to foresee for the very reason that they run counter to all of that accumulated intelligence. Even today, long after the facts, it is difficult to make an analytical, intelligence-based case (1) that when a crisis erupts in the Soviet Union, the Communist Party will peacefully give up power, or (2) that Saddam Hussein is telling the truth and has no WMD on hand.

As unsatisfactory as this standard is, other metrics are not much better. For example, a batting average could be constructed over time—for an issue, for an office, for an agency, for a product line. Or the quality of intelligence could be assessed on the basis of the number of products produced—estimates, analyses, images. But these measures are inadequate, too. Furthermore, they are not meant to be as frivolous as they seem. They are meant to give a feel for the difficulty of assessing what is good intelligence.

However, producing good intelligence is not some sort of Holy Grail that is rarely achieved. Good intelligence is often achieved. But one must distinguish between the steady stream of intelligence that is produced on a daily basis and the small amount within that daily production that stands out for some reason—its timeliness, the quality of its writing, its effect on policy. The view here—and it is one that has been debated with the highest intelligence officials—is that effort is required to produce acceptable, useful intelligence on a daily basis, but that producing exceptional intelligence is much more difficult and less frequently achieved. A conflict arises between the goal of consistency and the desire to be exceptional. An entire intelligence community cannot be exceptional all the time, but it does hope to be consistently helpful to policy. Consistent intelligence and exceptional intelligence are not one and the same. (As a cynic once said, “Only the mediocre are at their best all the time.”) Consistency is not a bad goal, but it allows analysis to fall into a pattern that lulls both the producer and the consumer. Thus, for all that is known about the distinctive characteristics of good intelligence, it remains somewhat elusive in
reality, at least as a widely seen daily phenomenon. But, for analysts, that is one of the positive challenges of their profession.

In the aftermath of 9/11 and Iraq WMD and after the promulgation of analytic standards, there still has not been closure on the key questions: How good is intelligence supposed to be, how often is it to be supplied, and on which issues? There are both professional and political answers to this question, but the inherent differences between them have not been resolved.

**Key Terms**

- analyst agility
- analyst fungibility
- analytic penetration
- analytical stovepipes
- assessments
- clientism
- competitive analysis
- confidence levels
- current intelligence
- estimates
- global coverage
- groupthink
- layering
- long-term intelligence
- mirror imaging
- national intelligence managers (NIMs)
- opportunity analysis
- politicized intelligence
- premature closure

**Further Readings**

The literature on analysis is rich. These readings discuss both broad, general issues and some specific areas of intelligence analysis that have been particularly important. The CIA has declassified many of its estimates on the Soviet Union and related issues. (See chap. 11.)


202 Intelligence: From Secrets to Policy
Copyright ©2015 by SAGE Publications, Inc. This work may not be reproduced or distributed in any form or by any means without express written permission of the publisher.


U.S. House Permanent Select Committee on Intelligence. Intelligence Support to Arms Control. 100th Cong., 1st sess., 1987.


U.S. Senate Select Committee on Intelligence. The National Intelligence Estimates A–B Team Episode Concerning Soviet Strategic Capability and Objectives. 95th Cong., 2d sess., 1978.


