A Framework for Strengthening U.S. Intelligence

BY LOCH K. JOHNSON

The main purpose of intelligence is to provide accurate, timely, and comprehensive information to the president and other policymakers to inform decision making. The task of providing useful information to government officials is a complex matter with many opportunities for error. Uncertainty and ambiguity dominate the environment in which key decisions are made. Accordingly, the numerous pitfalls that exist in the conduct of intelligence make some degree of failure inevitable.¹ Despite the inherent impossibility of perfect intelligence, reforming U.S. intelligence agencies can improve their performance and reduce the frequency of failure.

The U.S. intelligence community faces new challenges as its most pressing targets—particularly terrorist organizations—are structured to elude many of the tools of information-gathering that have proven successful in the past. Weaknesses exist in each step of the intelligence cycle, from planning and direction to collection, processing, analysis, and dissemination.² The mobilization of U.S. intelligence against these new threats requires not only redirected resources toward increased human intelligence but also a realignment of attitudes within and among the intelligence bureaucracies. The U.S. intelligence apparatus is constrained by miscommunication between analysts and policymakers resulting from sourcing, packaging, and sometimes distorting information. The intelligence shortcomings in advance of the September 11 attacks and the war in Iraq offer lessons for reform. Investments in new sources of human intelligence and data-mining can help boost U.S. information-gathering capabilities, though genuine intelligence reform will only be

Loch K. Johnson is Regents Professor of Public and International Affairs at the University of Georgia. He was a staff member of the U.S. Senate’s Church Committee on intelligence reform.
possible if the national director of intelligence is invested with the authority to override the bureaucratic turf wars among U.S. intelligence agencies.

The Intelligence Cycle

The planning and direction phase must account for a world with 191 states and a plethora of groups, factions, and gangs—some of which have adversarial relationships with the United States. Speaking just after the end of the Cold War, R. James Woolsey, director of central intelligence (DCI) during the Clinton administration, observed that, “We live now in a jungle filled with a bewildering variety of poisonous snakes.” At some point the degree of danger posed by an adversary can become painfully evident, as in the case of al-Qaeda after its attacks against New York City and Washington, D.C., on September 11, 2001. Unfortunately, no one can predict exactly when and where danger will strike, in part because we live in a world filled with secrets and mysteries.

By secrets, intelligence experts refer to information the United States might be able to discern even though it is concealed by another nation or group. For example, the numbers of Chinese tanks and nuclear submarines are discoverable but concealed by the Chinese government. In contrast, mysteries are events no one can know about until they happen because they lie beyond the limited human capacity to foresee. For example, no one knows who will be the next president of Russia. As former Secretary of State Dean Rusk liked to say, “Fate has not given mankind the capacity to pierce the fog of the future.”

Within this environment, intelligence agencies are faced with the task of determining intelligence priorities, a process known as threat assessment. Experts and policymakers gather periodically to evaluate the perils that confront the United States and establish a ladder of priorities from the most dangerous (Tiers 1A and 1B) to the least (Tier 4). Bias and guesswork enter the picture, along with the limitations caused by the uncertainty that surrounds the future. Where should one place China in the threat assessment? What about Russia, or Cuba? The outcome of these debates shapes the priorities for some $44 billion worth of intelligence spending each year. It also determines the areas U.S. spies will infiltrate, sets the orbits for surveillance satellites, and establishes the flight patterns of reconnaissance aircraft.

To improve the threat assessment process, the United States has undertaken nine major inquiries into its intelligence apparatus since the end of the Cold War. Each has concluded that policymakers failed to clarify during the
planning-and-direction phase of the intelligence cycle exactly what kinds of information they needed. Consequently, intelligence officers often remain ignorant of the data desired by policy officials, who in turn tend to assume that the intelligence agencies will divine the issues that await action at the White House, the State Department, and other important offices in Washington.

Among policy officials, the president and his top aides are the most important consumers of intelligence in the executive branch. These aides include members of the cabinet who deal with foreign and national security issues, along with the staff of the National Security Council (NSC). These men and women are pulled in many different directions by the demands of their daily schedules. As a result, they are reluctant to devote much time, if any, to updating their intelligence priorities.

Adding to this problem is spotty communication between analysts and decision makers. Sometimes NSC staffers, on the job for a year or more, have never spoken with experienced intelligence analysts on the National Intelligence Council who cover the same areas. This breakdown in communication stems from inadequate liaison relationships between the government’s policy departments and the intelligence agencies. The lack of synchronization causes frustration on both sides. All too often policymakers scrawl “irrelevant” or “OBE” (overtaken by events) in ink across intelligence reports.

The collection phase, which follows planning and direction in the intelligence cycle, faces challenges as well. Even a superpower like the United States is unable to cover the globe with expensive surveillance platforms (hardware), such as reconnaissance aircraft, satellites, and ground-based listening posts. During the Cold War, satellite photography monitored the missiles and armies of opponents, rendering a surprise attack like Pearl Harbor unlikely. Today however, cameras on satellites and airplanes are unable to peer inside al-Qaeda tents or into the deep underground caverns where North Korea constructs nuclear weapons. Though they comprise a high percentage of the funds allocated in the annual intelligence budget, costly hardware is of questionable value in tracking many contemporary U.S. security concerns.

Many of the best contributions from spy machines come from relatively inexpensive unmanned aerial vehicles, notably the Predator, which has proven effective at scouring the Iraqi and Afghan countryside in search
of insurgents. On occasion, the far more costly surveillance satellites have demonstrated their value by intercepting revealing telephone conversations among terrorists and other enemies (a method known as signals intelligence, the capture of communications from one person or group to another). Moreover, satellite images of Russian and Chinese missile sites, or North Korean troop movements, remain valuable to the security of the United States. Still, in the case of terrorism, it would be more advantageous to have a human agent well placed inside the upper reaches of al-Qaeda. Such an agent, or asset, would be worth a dozen multibillion-dollar satellites.

Yet human intelligence has its limitations as well. Against closed societies like North Korea, Iran, and Saddam Hussein’s Iraq, local assets are difficult to recruit. This is especially so because the United States focused for decades on the communist world and largely ignored the study of the languages, history, and culture necessary to operate in such places as the Middle East and Asia. Few U.S. citizens have mastered the nuances of Pashto, Arabic, or Farsi; fewer still are willing to work in perilous locations overseas for government wages.

Even if successfully recruited, indigenous assets can be unreliable. They are known to fabricate reports, sell information to the highest bidder, and scheme as false defectors or double-agents. Intelligence assets are not boy scouts or nuns; they are often driven by avarice and travel without moral compasses. “Curveball,” the prophetically codenamed German agent, provides a typical illustration of the risks involved in human intelligence. Spying inside Iraq in 2002, Curveball convinced the German intelligence service that weapons of mass destruction (WMD) existed in Saddam’s regime. The Central Intelligence Agency, in turn, took the bait through its liaison with the Germans.

Not every human intelligence asset turns out to be as deceptive as Curveball. Now and then a foreign spy provides extraordinarily useful information to the United States, as did the Soviet military intelligence officer Oleg Penkosky during the Cold War. Information from Col. Penkosky, coupled with photographs taken by U-2 reconnaissance aircraft, helped the CIA identify the presence of Soviet nuclear missiles in Cuba in 1962. With occasional successes like Penkosky in mind, the United States and most other countries continue their search for reliable and productive assets, even if the cost-benefit ratio has been disappointing.
Whether collected by machines or human agents, intelligence must be converted into usable information. For example, intercepted telephone conversations in Farsi must be translated into English. Messages may have to be decoded. This is done during the processing phase of the intelligence cycle. Each day, over four hundred satellite images, along with thousands of telephone intercepts, some in difficult codes, are collected by intelligence agencies. Yet the United States lacks sufficient translators, photo-interpreters, and code-breakers. In response to a query about the major problems facing U.S. intelligence, a recent director of the National Security Agency (NSA), Vice Admiral J.M. McConnell, identified three: “processing, processing, and processing.”

As the public now knows, the day before the September 11 attacks the NSA intercepted a telephone message in Farsi from a suspected al-Qaeda operative. The message, translated on September 12, proclaimed, “Tomorrow is zero hour.” As it stands, the vast majority of information gathered by the intelligence agencies is never examined. This is a supreme challenge for the government’s information technology specialists—improving the capacity of the United States to mine intelligence data more rapidly, separating the noise from the vital signals that decision makers need to know.

The heart of the intelligence cycle is the analysis phase, where the task is to bring insight to the information that has been collected and processed. The method is straightforward: hire qualified people to sift through all the available information in an attempt to predict what events may happen next in the world. Given the limitations of human forecasting, Dean Rusk suggested that all intelligence reports ought to start off with the caveat: “Damned if I know, but if you want our best guess, well, here it is.”

The intelligence cycle concludes with the dissemination phase. Perhaps the greatest paradox of U.S. intelligence is that so much effort and funding go into gathering information for policymakers only for them to ignore it. Some of the best assistant secretaries of defense and state have conceded that they spent, at best, five minutes a day scanning intelligence reports; they were simply too overwhelmed with other obligations. Officials even higher in the policy hierarchy have even less time read intelligence reports. The first challenge of dissemination, then, is to catch the attention of busy leaders, which is why marketing is a critical part of the intelligence cycle.

In marketing their products to consumers, the intelligence agencies confront several potential obstacles. Policymakers may choose to manipulate intelligence to fit their own political views or ideological predispositions—distor-
tion by politicization. Intelligence officers themselves may succumb to the temptation to slant information to suit the needs of policymakers as a way of advancing their career, delivering “intelligence to please.” Fortunately, analysts rarely succumb to this temptation, because most of them are imbued with a sense of professional ethics that shuns twisting information to please politicians.

More common is politicization on the consumer side, when policymakers bend the facts. Speaking truth to power is a notoriously difficult endeavor. Those in power often do not want to hear information that runs counter to their policy preferences; hence, they sometimes distort intelligence reports. Decision makers may cherry-pick snippets of information and analysis from intelligence reports that uphold their stated policy positions, ignoring contrary facts or conclusions. More blatant still, government officials have been known to discount entire intelligence reports, as President Lyndon B. Johnson did with CIA analyses that provided a dismal prognosis for U.S. military success in the Vietnam War, or as the second Bush administration did with CIA reports that found no connections between al-Qaeda and Saddam Hussein’s regime in Iraq. In such instances, the unenviable but vital responsibility of intelligence managers is to call policy officials to account for their distortions, publicly if necessary.

As this examination of the intelligence cycle indicates, many opportunities for error and distortion present themselves as intelligence makes its way from the field into the hands of decision makers. Nonetheless, U.S. intelligence agencies have some advantages in their quest for information. Willing to spend vast sums of money on espionage, the United States enjoys the largest, most sophisticated information-gathering apparatus in the world. This bureaucracy brings in a torrent of information from across the globe, some of which has been invaluable for defending U.S. overseas interests and homeland security. The intelligence agencies are expert, as well, in packaging and delivering their assessments of international affairs to the right people in government in a timely manner. Even so, intelligence failures continue to happen. Perhaps nothing illustrates this reality so clearly as two recent cases: the attacks of September 11, 2001, and the misjudgment about the presence of weapons of mass destruction in Iraq.

The 9/11 Intelligence Failure

U.S. intelligence agencies performed in a more credible manner to warn the nation of the terrorist threat before September 11, 2001, than is usually acknowledged. As early as 1995, the CIA’s Counterterrorism Center (CTC)
cautioned the White House that “aerial terrorism seems likely at some point—filling an airplane with explosives and dive-bombing a target.” The warning erred only in its failure to comprehend that hijacked commercial aircraft, with their highly volatile jet fuel, would be powerful missiles without added explosives. Analysts in the CTC had good reason to be concerned about aerial terrorism during the 1990s. Frequent reports had surfaced in the media about terrorist schemes to fly an airplane into the Eiffel Tower or into CIA headquarters. The CTC’s warnings on this topic appeared in high policy circles with regularity between 1995 and 2001.

Yet the CTC never provided officials with precise information about the timing or location of the anticipated hijackings, the kind of actionable intelligence that would have allowed U.S. authorities to intercept the terrorists before they boarded the airplanes. Moreover, the intelligence agencies flooded officials with dire warnings about other possible threats, from trucks filled with dynamite exploding in urban tunnels to attacks against the nation’s railroad system, crops, livestock, computer infrastructure, and water supplies. Missing in these reports was a sense of priority or probability among the threats, as well as the degree of specificity necessary to take timely protective measures.

Moreover, government inquiries have discovered that the intelligence agencies failed to coordinate and act on the few shards of specific information they did have regarding the September 11 operatives. For instance, the agencies proved unable to track two of the nineteen terrorists, despite warnings from the CIA to the Federal Bureau of Investigation about the terrorists’ arrival in San Diego. Furthermore, the FBI failed to respond to warnings from its own agents in Phoenix and Minneapolis about suspicious flight training undertaken by foreigners in those cities. And the Department of Defense smothered warnings from the “Able Danger” group of military intelligence officers who had apparently discovered the presence of sixty foreign terrorists in the United States almost two years before the September 11 attacks. Among the sixty were four of the September 11 hijackers, including their Egyptian-born leader, Mohamed Atta.

At a deeper level, September 11 was an intelligence failure because the CIA had no assets within al-Qaeda, because the National Security Agency (NSA) fell far behind on translating relevant signals intelligence intercepts involving suspected terrorists, and because all of the intelligence agencies lacked sufficient language skills and understanding about nations in the Middle East and South Asia and the objectives and likely motivations of al-Qaeda.
Yet September 11 was more than an intelligence failure; it was a policy failure too. Despite the CIA’s warnings about aerial terrorism, for example, neither the Clinton nor the second Bush administrations took meaningful steps to tighten airport security, warn pilots, seal off cockpits, field air marshals, or even alert top officials in the Department of Transportation about the terrorist danger.

**Iraqi Weapons of Mass Destruction**

The intelligence failures regarding Iraqi weapons of mass destruction were in some ways even more troubling than those that preceded the September 11 attacks. The National Intelligence Estimate (NIE) of October 2002 concluded, as did most intelligence agencies and outside analysts, that unconventional weapons were most likely present in Iraq. This assessment was based on several inaccurate sources of information. First, since the intelligence community had no significant human assets in Iraq during the interwar years, analysts in the United States extrapolated from what they knew when the United States last had “boots on the ground”—after the first Persian Gulf War in 1991. At that time, the CIA learned that its pre-war estimates regarding Iraqi WMD were inaccurate; Iraq’s weapons program had advanced far beyond what the CIA’s analysts had projected. After U.S. troops departed Iraq in 1991, the CIA lacked reliable sources on the ground. Thus, in the run-up to the second Persian Gulf War, CIA analysts compensated for earlier underestimates by overestimating the probability of Iraqi WMD.

The available human intelligence proved problematic. Reports from the German asset Curveball, whose reliability was vouched for by the Germans, also factored into the CIA’s miscalculations. Only recently have the Germans conceded that the Iraqi exile was in fact lying. Moreover, the confessions of a captured al-Qaeda member, Ibn al-Shaykh al-Libi, interrogated by the Defense Intelligence Agency (DIA), also proved to be fabrications. In addition, the Iraqi National Congress, led by another Iraqi exile, Ahmed Chalabi, claimed knowledge of Iraq’s activities and informed U.S. intelligence agencies and the second Bush administration that Saddam Hussein was pursuing nuclear weapons. Chalabi’s reliability has since been called into question. Critics maintain that his purpose may have been chiefly to push for a U.S. invasion so that he might advance his personal political agenda and replace Hussein as president of Iraq.

CIA analysts were also aware that British intelligence was concerned about the existence of Iraqi WMD. Yet British government inquiries into this matter, notably the Butler Report, disclosed that the worries of British intelligence
analysts focused on a possible Iraqi use of tactical chemical or biological weapons on the battlefield by Hussein if he faced an invasion, as opposed to strategic WMD that could directly strike the United Kingdom, the United States, or even their military forces in the Middle East away from the battlefield.

It is often claimed that the second Bush Administration pressured intelligence analysts to write an NIE that emphasized the probability of weapons of mass destruction in Iraq. Such a finding would have supported a policy to invade Iraq and overthrow Hussein’s regime, which some argue was the administration’s desired course of action regardless of whether the Iraqi dictator had an unconventional weapons program. Vice President Dick Cheney visited CIA headquarters an unprecedented eight times prior to the publication of the 2002 NIE, pressing analysts on their conclusions whenever they strayed from his conviction that Iraq was pursuing capabilities in weapons of mass destruction. The CIA analysts whom Cheney visited assert, however, that they felt no sense of intimidation by his presence; on the contrary, they were pleased to have such unusual high-level attention paid to their work.13

Then-Secretary of State Colin Powell also visited with CIA officials to probe the strength of evidence concerning WMD in Iraq, especially on the eve of his appearance before the United Nations on February 3, 2003, to make the case that Saddam Hussein was a great danger. During his preparation, Powell encountered some disagreement among intelligence analysts, including dissent within his own intelligence organization, the Department of State’s Bureau of Intelligence and Research (INR). He also learned of other pockets of dissent inside the Department of Energy’s intelligence unit and the Air Force’s intelligence service. Yet, the analytic behemoths of the intelligence community, most notably the CIA and the DIA, maintained that Iraq probably did possess weapons of mass destruction. Their reasoning pivoted on Iraq’s purchase of 60,000 high-strength aluminum tubes, which, they argued, seemed designed for a uranium centrifuge and a nuclear weapons program.14 Moreover, then-DCI George Tenet, vigorously backed the majority opinion. Secretary Powell deferred to this powerful coalition, even though analysts in INR and the Department of Energy pointed out that the aluminum tubes were more likely combustion chambers for conventional rockets. For the most part, though, these were internal disputes that took place outside the hearing of the American public. The dissenting views of the smaller agencies were largely dismissed by the larger and more powerful agencies.

President George W. Bush himself questioned Tenet directly about his confidence in the October 2002 NIE. As reported by Bob Woodward of the
The Washington Post, the intelligence director assured the president that the presence of weapons of mass destruction in Iraq was a “slam dunk.” A careful reading of the NIE indicates, however, that the analysts who wrote the assessment hardly claimed perfect knowledge about the state of Saddam Hussein’s unconventional weapons program. The odds favored finding WMD, but analysts inserted caveats into the estimate regarding the “softness” of the data.

This softness is precisely what Tenet should have underscored for the president. The DCI should have pointed out that the NIE was not a definitive report—indeed, it was a rushed job prepared in only three weeks—that additional on-the-ground fact-finding was sorely needed, and that the CIA felt uneasy about the human intelligence reporting provided by Curveball, al-Libi, and Chalabi. A briefing along these lines from Tenet to the president would have highlighted the need for a delay in the invasion plans until UN weapons inspectors had cleared up the intelligence ambiguities. Instead, the White House appears to have been all too ready to accept the convenient findings of some intelligence agencies that happened to run parallel to its own policy ambitions, namely, regime change in Iraq. As a result, Tenet evidently fell into a trap that awaits every U.S. spymaster: the snare of White House politics. Caught up in the administration’s euphoria for war against Saddam Hussein, the pursuit of democracy in the Middle East, and a demonstration of U.S. military might as a warning to adversaries, Tenet’s reassurance provided an intelligence linchpin for the president to confirm his argument in favor of an Iraqi invasion.

Earlier, Tenet had failed to set the record straight at another important moment in the WMD debate. Inserted into the State of the Union address in 2003 was an assertion that Iraq had attempted to purchase 500 tons of yellowcake uranium from Niger, indicating that Hussein was indeed pursuing a nuclear weapons program. The CIA looked into this allegation by sending former U.S. Ambassador to Niger Joseph C. Wilson IV to make direct inquiries. The ambassador, however, found no evidence to support the hypothesis and the CIA reported this conclusion to the deputy national security advisor, Steven H. Hadley, well in advance of the State of the Union address. Yet the speech included the yellowcake claim anyway, which was now cloaked with the legitimacy of the president’s own word in a nationally televised address. Tenet later claimed that he had not seen an advance copy of the speech and...
was therefore unable to amend the text. The “eighteen words” regarding Nigerian yellowcake have since become a focus of war critics, as has the outing of Wilson’s wife, Valerie Plame, as an undercover CIA operative.

The unwillingness of the CIA to confront policy officials who exaggerated intelligence reporting has been perhaps the most disquieting aspect of the WMD intelligence debates. Throughout these distortions, the CIA mostly stood mute. One exception occurred when analysts complained publicly, through anonymous media leaks, that Vice President Cheney was in error to insist that a significant tie existed between al-Qaeda and the Iraqi government. Intelligence reporting had concluded that no such connection existed, though CIA analysts warned that a bond might be forged between global jihadists and Baghdad—or insurgent remnants—if the West were to invade Iraq. Despite the CIA’s findings to the contrary, Cheney continued to state publicly that al-Qaeda and the Hussein regime were secretly allied.

Proposals for Reform

The American public must come to understand that intelligence agencies, like any human enterprise, will always have their share of failures. Nevertheless, much can be done to reduce the chance of mistakes. At the planning and direction phase, policy officials must define information needs with greater precision. Collection has been too broad and requires a sharper focus. What exactly do decision makers need to know? On what specific topics should the intelligence agencies focus? The tasking of intelligence agencies is often vaguely spelled out, if at all, and the result is an overly diffuse global intelligence collection effort. The president should issue a quarterly National Security Council Intelligence Directive that updates the administration’s threat assessment and current intelligence needs. The president should insist on specific directives—for example, “Track all uranium shipments from Niger, worldwide”—rather than vague orders like “Provide the Secretary of Defense with intelligence on Niger.”

Within the collection phase, renewed concentration on human intelligence is critical. Since 1947, technical intelligence such as signals intelligence and satellite imagery has dominated the U.S. intelligence budget at the expense of human intelligence. The intelligence budget is just beginning to shift funds toward human intelligence. Funding, however, is only the first step. Spy rings are relatively inexpensive to set up; the more difficult challenge is to develop among intelligence officers the language skills and knowledge of foreign cultures necessary for the effective recruitment of assets abroad. This effort cannot succeed overnight; it is bound to take at least ten to fifteen
years. The creation of government scholarships to attract top students into the intelligence agencies, such as the Pat Roberts Intelligence Scholars Program, is a step in the right direction. In return for service in an intelligence agency for a period of time, usually two to three years, the government covers college tuition for students studying foreign languages and cultures.

The intelligence agencies must also do more to recruit U.S. citizens with ethnic heritages germane to strategic areas such as the Middle East, South Asia, and other regions largely ignored during the Cold War. For example, Arab-Americans, who face enhanced scrutiny, need to be recruited into the intelligence agencies in much larger numbers and should not be shunned as prima facie security risks. Once cleared through the normal background security checks, Arab-Americans who wish to work in the government should be actively recruited.

Successful recruitment will also require better salaries, since the private sector is also seeking workers with backgrounds in foreign languages and cultures. Although public sector positions pay less than private sector jobs, many top college students would rather serve the United States in the struggle against global terrorism and other threats than hunt down obscure cases in the library of a law firm. Reducing the financial tradeoffs necessary to making such a career choice would go a long way to ensuring that more talented young people are brought into government service.

Equally important will be efforts to expand the CIA’s use of what are called NOCs—U.S. citizens under non-official cover—who operate within a local society, say, as an investment banker in Egypt, a hotel manager in Dubai, or an oil rigger in Bahrain. Moving intelligence officers out of embassies and into the field will make them more likely to meet potential assets and understand the undercurrents of foreign societies. In light of the added hardships and risks of a NOC career, salaries and bonuses should be considerably higher for those who select this path, and more effort will have to be put into crafting their covers, their methods of communication with CIA headquarters, and their rescue if they find themselves in jeopardy overseas.

Furthermore, the United States must examine anew the relationship between the FBI and the Foreign Intelligence Surveillance Court. Established by the Foreign Intelligence Surveillance Act (FISA) of 1978, this court reviews warrant requests for national security wiretaps and other forms of electronic surveillance, as well as physical searches. As a safeguard against intelligence agencies overstepping their powers, as occurred with the FBI in the 1960s and is a subject of current inquiry with the NSA, the FISA Court stands as
a vital check on the merits of surveillance requests. Yet steps must also be taken to ensure that warrants can be acquired with dispatch in properly documented cases of national security threats. This did not happen in the case of a suspected al-Qaeda member in Minneapolis prior to the September 11 attacks. When information is collected by the CIA or other intelligence agencies regarding terrorists traveling toward or operating within the United States, the FBI must be alerted quickly and clearly so that it can conduct follow-up surveillance.

At the processing phase, the intelligence agencies are behind the curve on data-mining. Here, too, the federal government must pay higher salaries and bonuses to attract top talent who can assist the intelligence agencies in overcoming information technology deficiencies. By setting up a quasi-government company in Silicon Valley called “In-Q-Tel,” the CIA has already reached out to some of the nation’s top computer talent. Further outreach and more money are critical. The intelligence agencies desperately need to bring in IT expertise to integrate their systems, while at the same time enhancing firewalls to protect sensitive intelligence from theft by outside hackers and foreign intelligence services. The FBI in particular has lost credibility among Capitol Hill appropriators, having spent over $580 billion on a non-functioning computer system. A reputable outsider recruited into a senior intelligence management position might be able to restore congressional confidence and attract the necessary appropriations to achieve seamless integration among intelligence agencies. The central technological challenge has two elements. First, as information is gathered by the intelligence agencies from around the world, sophisticated machine-sorting techniques are necessary to separate key signals from the high percentage of surrounding “noise” that streams into the secret agencies. Second, useful intelligence must be rapidly shared among the intelligence agencies in Washington, as well as with law enforcement and intelligence officials at the state and local levels. This requires an effective integration of computer networks, both horizontally (in the nation’s capital) and vertically (downward to state and local counterterrorism officials).

During the analytical phase, intelligence officers will need to be more careful about including caveats and nuances in their reporting, as well as making clear just how good—or bad—their sources are. For their part, the president and other policymakers must let it be known to intelligence managers and analysts that vague generalities will not be accepted in NIEs and other reports.
One high-level intelligence briefer told the Aspin-Brown Commission in 1996 that North Korea “might have one or two nuclear weapons or it might not have any.”\(^\text{18}\) Missing was a sense of what analysts believed were the probabilities of a North Korean nuclear weapon within the next year. When an analyst presents a list of threats without any sense of which ones are most likely, the result is paralysis among policymakers.

Intelligence collectors and analysts must also be more thorough in vetting their sources. When the Germans balked at allowing the CIA to conduct its own interviews with the asset Curveball, the CIA’s analysts should have downgraded the quality of this source to a low level or declined to use the source at all. Important, too, are efforts to ensure that policymakers understand the reasons behind dissents voiced by intelligence agencies or individual analysts. Their arguments must be showcased, along with the prevailing majority opinions, so that policymakers have a full understanding of the key points of contention. During the Iraqi WMD debate, the contrary views of the Department of Energy, the State Department’s Bureau of Intelligence and Research, and the Air Force were insufficiently underscored.

At the dissemination phase, analysts and intelligence managers should be trained to resist more effectively pressures from policymakers to “cook” intelligence. A self-imposed wall must separate analysts from an administration’s policy ambitions. Further, analysts must be determined to set the record straight for the public if intelligence reports are twisted for policy purposes by government officials. Intelligence officers, particularly the nation’s intelligence director, must be brutally candid with respect to the limits of the reports they have prepared, warning the president and other officials about the extent to which conclusions are based on conjecture more than empirical indicators, such as unambiguous imagery. Those parts of reports that are largely speculative must be carefully delineated from the fact-based findings.

Fresh incentives can be established to encourage the maintenance of a wall between analysts and policymakers, one that will not prevent them from communicating with one another but that erects a barrier against the coloration of intelligence to suit policy objectives. One stick would be to fire analysts who violate the norms of objectivity. Carrots would include promotions, bonuses, and special recognition to those analysts who display exemplary professional conduct. Though rarely used, A-team, B-team exercises in competitive analysis are a useful means for validating objectivity, as long as the teams are staffed with unbiased experts. Above all, the integrity of the analytic process depends on the recruitment of honest men and women into the intelligence agencies.
Critical, too, is the need for constructing better bridges between policymakers and intelligence agencies. The best approach is for the agencies to gain permission to place liaison officers in policy departments so they can attend staff meetings, periodically discuss with decision makers their information needs, and learn from the inside how they can help with timely factual information and objective analysis. With this approach, intelligence is more likely to be relevant to the immediate agendas of government leaders.

No intelligence reform proposal is more important than putting in place a Director of National Intelligence (DNI) with full budget and appointment powers over all intelligence agencies, a true leader with a broad perspective on spending, planning, collection, processing, analysis, and dissemination—someone who could overcome the stovepiped autonomy of the individual intelligence agencies that has plagued them since 1947. The creation of a strong intelligence chief has been the core recommendation of major intelligence reform commissions since 1949, most recently of the 9/11 Commission in 2004.

Over the years, the Department of Defense (DoD) has skillfully resisted the idea of creating a DNI, jealously guarding its military intelligence prerogatives against the possible encroachment of a civilian intelligence chief. Finally, in 2004, with the passage by Congress of the Intelligence Reform and Terrorism Prevention Act, the 9/11 Commission seemed to have achieved the impossible: the establishment of a robust DNI. Yet a close look at the statute reveals that the DoD and its allies in Congress have managed to dilute and obfuscate the authority of the new intelligence director. As a result, the inaugural DNI, Ambassador John D. Negroponte, faces an uphill battle to consolidate his control over the entire intelligence establishment. His most important challenge will be to persuade the intelligence agencies to pool their information more effectively. In light of the DoD’s opposition to a strong DNI, the ambassador’s chances for gathering together the reins of a set of agencies so obviously fissile appear slim—unless President Bush or his successor demands a genuine leader for U.S. intelligence, not just a figurehead.

Over the objections of the secretary of defense, a president would have to insist that the DNI be given the authority to hire and fire all intelligence personnel, as well as determine—in consultation with their senior management teams—the budgets of each agency. With these prerogatives, the DNI would finally serve as a hoop to bind together the fifteen staves of the intelligence “community.”

President Bush is an unlikely candidate to force this issue given distractions from the wars in Iraq and Afghanistan, the campaign against global ter-
rorism, and his dependence on Secretary of Defense Donald H. Rumsfeld. Furthermore, the president has never exhibited much interest in intelligence reform. His administration initially opposed a joint congressional investigation into the intelligence errors related to the attacks of September 11. Then, once the panel was formed, the administration stonewalled the inquiry. The White House also tried to block the creation of the 9/11 Commission, but finally acceded to pressures from the families of the September 11 victims and grudgingly cooperated with its investigation.

The absence of consistent presidential leadership to strengthen the U.S. intelligence shield is unfortunate. The need to bring unity and coordination to the nation’s intelligence agencies is a matter of enormous importance. The security of the United States rides heavily on the outcome of this struggle now unfolding in Washington. If the government proves unwilling or unable to make the necessary improvements to protect the nation, citizens will have to demand change through public lobbying or, if necessary, the ballot box.

NOTES
4 Dean Rusk, interview with author, Athens, Georgia, 21 February 1988.
6 Dean Rusk, interview with author, Athens, Georgia, 21 February 1988).
7 See, for example, Loch K. Johnson, Bombs, Bugs, Drugs, and Thugs: Intelligence and America’s Quest for Security (New York: New York University Press, 2000), 194.
18 Member of the Aspin-Brown Commission, interview with author, Washington, DC 22 March 1997.
19 See, for example, the critique by John Brennan, “Is This Intelligence?” Washington Post, 20 November 2005, B1.