OVERVIEW OF THE REPORT

OVERVIEW OF THE REPORT

INTRODUCTION

On the brink of war, and in front of the whole world, the United States government asserted that Saddam Hussein had reconstituted his nuclear weapons program, had biological weapons and mobile biological weapon production facilities, and had stockpiled and was producing chemical weapons. All of this was based on the assessments of the U.S. Intelligence Community. And not one bit of it could be confirmed when the war was over.

While the intelligence services of many other nations also thought that Iraq had weapons of mass destruction, in the end it was the United States that put its credibility on the line, making this one of the most public—and most damaging—intelligence failures in recent American history.

This failure was in large part the result of analytical shortcomings; intelligence analysts were too wedded to their assumptions about Saddam's intentions. But it was also a failure on the part of those who collect intelligence—CIA's and the Defense Intelligence Agency's (DIA) spies, the National Security Agency's (NSA) eavesdroppers, and the National Geospatial-Intelligence Agency's (NGA) imagery experts.* In the end, those agencies collected precious little intelligence for the analysts to analyze, and much of what they did collect was either worthless or misleading. Finally, it was a failure to communicate effectively with policymakers; the Intelligence Community didn't adequately explain just how little good intelligence it had—or how much its assessments were driven by assumptions and inferences rather than concrete evidence.

Was the failure in Iraq typical of the Community's performance? Or was Iraq, as one senior intelligence official told the Commission, a sort of "perfect storm"—a one-time breakdown caused by a rare confluence of events that conspired to create a bad result? In our view, it was neither.

---

* While we have attempted to write this report in a way that is accessible to those not acquainted with the world of intelligence, we have included a primer on the U.S. Intelligence Community at Appendix C of this report for readers who are new to the subject.

The failures we found in Iraq are not repeated everywhere. The Intelligence Community played a key role, for example, in getting Libya to renounce weapons of mass destruction and in exposing the long-running A.Q. Khan nuclear proliferation network. It is engaged in imaginative, successful (and highly classified) operations in many parts of the world. Tactical support to counterterrorism efforts is excellent, and there are signs of a boldness that would have been unimaginable before September 11, 2001.

But neither was Iraq a "perfect storm." The flaws we found in the Intelligence Community's Iraq performance are still all too common. Across the board, the Intelligence Community knows disturbingly little about the nuclear programs of many of the world's most dangerous actors. In some cases, it knows less now than it did five or ten years ago. As for biological weapons, despite years of Presidential concern, the Intelligence Community has struggled to address this threat.

To be sure, the Intelligence Community is full of talented, dedicated people. But they seem to be working harder and harder just to maintain a *status quo* that is increasingly irrelevant to the new challenges presented by weapons of mass destruction. Our collection agencies are often unable to gather intelligence on the very things we care the most about. Too often, analysts simply accept these gaps; they do little to help collectors identify new opportunities, and they do not always tell decisionmakers just how limited their knowledge really is.

Taken together, these shortcomings reflect the Intelligence Community's struggle to confront an environment that has changed radically over the past decade. For almost 50 years after the passage of the National Security Act of 1947, the Intelligence Community's resources were overwhelmingly trained on a single threat—the Soviet Union, its nuclear arsenal, its massive conventional forces, and its activities around the world. By comparison, today's priority intelligence targets are greater in number (there are dozens of entities that could strike a devastating blow against the United States) and are often more diffuse in character (they include not only states but also nebulous transnational terror and proliferation networks). What's more, some of the weapons that would be most dangerous in the hands of terrorists or rogue nations are difficult to detect. Much of the technology, equipment, and materials necessary to develop biological and chemical weapons, for example, also has legitimate commercial applications. Biological weapons

themselves can be built in small-scale facilities that are easy to conceal, and weapons-grade uranium can be effectively shielded from traditional detection techniques. At the same time, advances in technology have made the job of technical intelligence collection exceedingly difficult.

The demands of this new environment can only be met by broad and deep change in the Intelligence Community. The Intelligence Community we have today is buried beneath an avalanche of demands for "current intelligence"—the pressing need to meet the tactical requirements of the day. Current intelligence in support of military and other action is necessary, of course. But we also need an Intelligence Community with *strategic* capabilities: it must be equipped to develop long-term plans for penetrating today's difficult targets, and to identify political and social trends shaping the threats that lie over the horizon. We can imagine no threat that demands greater strategic focus from the Intelligence Community than that posed by nuclear, biological, and chemical weapons.

The Intelligence Community is also fragmented, loosely managed, and poorly coordinated; the 15 intelligence organizations are a "Community" in name only and rarely act with a unity of purpose. What we need is an Intelligence Community that is *integrated*: the Community's leadership must be capable of allocating and directing the Community's resources in a coordinated way. The strengths of our distinct collection agencies must be brought to bear together on the most difficult intelligence problems. At the same time we need a Community that preserves diversity of analysis, and that encourages structured debate among agencies and analysts over the interpretation of information.

Perhaps above all, the Intelligence Community is too slow to change the way it does business. It is reluctant to use new human and technical collection methods; it is behind the curve in applying cutting-edge technologies; and it has not adapted its personnel practices and incentives structures to fit the needs of a new job market. What we need is an Intelligence Community that is flexible—able to respond nimbly to an ever-shifting threat environment and to the rapid pace of today's technological changes.

In short, to succeed in confronting today's and tomorrow's threats, the Intelligence Community must be transformed—a goal that would be difficult to meet even in the best of all possible worlds. And we do not live in the best of

worlds. The CIA and NSA may be sleek and omniscient in the movies, but in real life they and other intelligence agencies are vast government bureaucracies. They are bureaucracies filled with talented people and armed with sophisticated technological tools, but talent and tools do not suspend the iron laws of bureaucratic behavior. Like government bodies everywhere, intelligence agencies are prone to develop self-reinforcing, risk averse cultures that take outside advice badly. While laudable steps were taken to improve our intelligence agencies after September 11, 2001, the agencies have done less in response to the failures over Iraq, and we believe that many within those agencies do not accept the conclusion that we reached after our year of study: that the Community needs fundamental change if it is to successfully confront the threats of the 21st century.

We are not the first to say this. Indeed, commission after commission has identified some of the same fundamental failings we see in the Intelligence Community, usually to little effect. The Intelligence Community is a closed world, and many insiders admitted to us that *it has an almost perfect record of resisting external recommendations.*

But the present moment offers an unprecedented opportunity to overcome this resistance. About halfway through our inquiry, Congress passed the *Intelligence Reform and Terrorism Prevention Act of 2004*, which became a sort of a *deus ex machina* in our deliberations. The act created a Director of National Intelligence (DNI). The DNI's role could have been a purely coordinating position, with a limited staff and authority to match. Or it could have been something closer to a "Secretary of Intelligence," with full authority over the principal intelligence agencies and clear responsibility for their actions—which also might well have been consistent with a small bureaucratic superstructure. In the end, the DNI created by the intelligence reform legislation was neither of these things; the office is given broad responsibilities but only ambiguous authorities. While we might have chosen a different solution, we are not writing on a blank slate. So our focus has been in large part on how to make the new intelligence structure work, and in particular on giving the DNI tools (and support staff) to match his large responsibilities.

We are mindful, however, that there is a serious risk in creating too large a bureaucratic structure to serve the DNI: the risk that decisionmaking in the field, which sometimes requires quick action, will be improperly delayed. Balancing these two imperatives—necessary agility of operational execution

and thoughtful coordination of intelligence activities—is, in our view, the DNI's greatest challenge.

In considering organizational issues, we did not delude ourselves that organizational structure alone can solve problems. More than many parts of government, the culture of the Intelligence Community is formed in the field, where organizational changes at headquarters are felt only lightly. We understand the limits of organizational change, and many of our recommendations go beyond organizational issues and would, if enacted, directly affect the way that intelligence is collected and analyzed. But we regret that we were not able to make such detailed proposals for some of the most important technical collection agencies, such as NSA and NGA. For those agencies, and for the many other issues that we could only touch upon, we must trust that our broader institutional recommendations will enable necessary reform. The DNI that we envision will have the budget and management tools to dig deep into the culture of each agency and to force changes where needed.

This Overview—and, in far more detail, the report that follows—offers our conclusions on what needs to be done. We begin by describing the results of our case studies—which include Iraq, Libya, Afghanistan, and others—and the lessons they teach about the Intelligence Community's current capabilities and weaknesses. We then offer our recommendations for reform based upon those lessons.

Three final notes before proceeding. First, our main tasks were to find out how the Intelligence Community erred in Iraq and to recommend changes to avoid such errors in the future. This is a task that often lends itself to hubris and to second-guessing, and we have been humbled by the difficult judgments that had to be made about Iraq and its weapons programs. We are humbled too by the complexity of the management and technical challenges intelligence professionals face today. We recommend substantial changes, and we believe deeply that such changes are necessary, but we recognize that other reasonable observers could come to a different view on some of these questions.

Second, no matter how much we improve the Intelligence Community, weapons of mass destruction will continue to pose an enormous threat. Intelligence will always be imperfect and, as history persuades us, surprise can never be completely prevented. Moreover, we cannot expect spies, satellites, and analysts

to constitute our only defense. As our biological weapons recommendations make abundantly clear, all national capabilities—regulatory, military, and diplomatic—must be used to combat proliferation.

Finally, we emphasize two points about the scope of this Commission's charter, particularly with respect to the Iraq question. First, we were *not* asked to determine whether Saddam Hussein had weapons of mass destruction. That was the mandate of the Iraq Survey Group; our mission is to investigate the reasons why the Intelligence Community's pre-war assessments were so different from what the Iraq Survey Group found after the war. Second, we were not authorized to investigate how policymakers used the intelligence assessments they received from the Intelligence Community. Accordingly, while we interviewed a host of current and former policymakers during the course of our investigation, the purpose of those interviews was to learn about how the Intelligence Community reached and communicated its judgments about Iraq's weapons programs—not to review how policymakers subsequently used that information.

LOOKING BACK: CASE STUDIES IN FAILURE AND SUCCESS

Our first task was to evaluate the Intelligence Community's performance in assessing the nuclear, biological, and chemical weapons activities of three countries: Iraq, Afghanistan, and Libya. In addition, we studied U.S. capabilities against other pressing intelligence problems—including Iran, North Korea, Russia, China, and terrorism. We wanted a range of studies so we would not judge the Intelligence Community solely on its handling of Iraq, which was—however important—a single intelligence target. In all, the studies paint a representative picture. It is the picture of an Intelligence Community that urgently needs to be changed.

Iraq: An Overview

In October 2002, at the request of members of Congress, the National Intelligence Council produced a National Intelligence Estimate (NIE)—the most authoritative intelligence assessment produced by the Intelligence Community—which concluded that Iraq was reconstituting its nuclear weapons program and was actively pursuing a nuclear device. According to the exhaustive study of the Iraq Survey Group, this assessment was almost com-

pletely wrong. The NIE said that Iraq's biological weapons capability was larger and more advanced than before the Gulf War and that Iraq possessed mobile biological weapons production facilities. This was wrong. The NIE further stated that Iraq had renewed production of chemical weapons, including mustard, sarin, GF, and VX, and that it had accumulated chemical stockpiles of between 100 and 500 metric tons. All of this was also wrong. Finally, the NIE concluded that Iraq had unmanned aerial vehicles that were probably intended for the delivery of biological weapons, and ballistic missiles that had ranges greater than the United Nations' permitted 150 kilometer range. In truth, the aerial vehicles were not for biological weapons; some of Iraq's missiles were, however, capable of traveling more than 150 kilometers. The Intelligence Community's Iraq assessments were, in short, riddled with errors.

Contrary to what some defenders of the Intelligence Community have since asserted, these errors were *not* the result of a few harried months in 2002. Most of the fundamental errors were made and communicated to policymakers well before the now-infamous NIE of October 2002, and were not corrected in the months between the NIE and the start of the war. They were not isolated or random failings. Iraq had been an intelligence challenge at the forefront of U.S. attention for over a decade. It was a known adversary that had already fought one war with the United States and seemed increasingly likely to fight another. But, after ten years of effort, the Intelligence Community still had no good intelligence on the status of Iraq's weapons programs. Our full report examines these issues in detail. Here we limit our discussion to the central lessons to be learned from this episode.

The first lesson is that the Intelligence Community cannot analyze and disseminate information that it does not have. The Community's Iraq assessment was crippled by its inability to collect meaningful intelligence on Iraq's nuclear, biological, and chemical weapons programs. The second lesson follows from the first: lacking good intelligence, analysts and collectors fell back on old assumptions and inferences drawn from Iraq's past behavior and intentions.

The Intelligence Community had learned a hard lesson after the 1991 Gulf War, which revealed that the Intelligence Community's pre-war assessments had underestimated Iraq's nuclear program and had failed to identify all of its chemical weapons storage sites. Shaken by the magnitude of their errors,

intelligence analysts were determined not to fall victim again to the same mistake. This tendency was only reinforced by later events. Saddam acted to the very end like a man with much to hide. And the dangers of underestimating our enemies were deeply underscored by the attacks of September 11, 2001.

Throughout the 1990s, therefore, the Intelligence Community assumed that Saddam's Iraq was up to no good—that Baghdad had maintained its nuclear, biological, and chemical technical expertise, had kept its biological and chemical weapons production capabilities, and possessed significant stockpiles of chemical agents and weapons precursors. Since Iraq's leadership had not changed since 1991, the Intelligence Community also believed that these capabilities would be further revved up as soon as inspectors left Iraq. Saddam's continuing cat-and-mouse parrying with international inspectors only hardened these assumptions.

These experiences contributed decisively to the Intelligence Community's erroneous National Intelligence Estimate of October 2002. That is not to say that its fears and assumptions were foolish or even unreasonable. At some point, however, these premises stopped being working hypotheses and became more or less unrebuttable conclusions; worse, the intelligence system became too willing to find confirmations of them in evidence that should have been recognized at the time to be of dubious reliability. Collectors and analysts too readily accepted any evidence that supported their theory that Iraq had stockpiles and was developing weapons programs, and they explained away or simply disregarded evidence that pointed in the other direction.

Even in hindsight, those assumptions have a powerful air of common sense. If the Intelligence Community's estimate and other pre-war intelligence had relied principally and explicitly on inferences the Community drew from Iraq's past conduct, the estimate would still have been wrong, but it would have been far more defensible. For good reason, it was hard to conclude that Saddam Hussein had indeed abandoned his weapons programs. But a central flaw of the NIE is that it took these defensible assumptions and swathed them in the mystique of intelligence, providing secret information that seemed to support them but was in fact nearly worthless, if not misleading. The NIE simply didn't communicate how weak the underlying intelligence was.

This was, moreover, a problem that was not limited to the NIE. Our review found that *after* the publication of the October 2002 NIE but *before* Secre-

tary of State Colin Powell's February 2003 address to the United Nations, intelligence officials within the CIA failed to convey to policymakers new information casting serious doubt on the reliability of a human intelligence source known as "Curveball." This occurred despite the pivotal role Curveball's information played in the Intelligence Community's assessment of Iraq's biological weapons programs, and in spite of Secretary Powell's efforts to strip every dubious piece of information out of his proposed speech. In this instance, once again, the Intelligence Community failed to give policymakers a full understanding of the frailties of the intelligence on which they were relying.

Finally, we closely examined the possibility that intelligence analysts were pressured by policymakers to change their judgments about Iraq's nuclear, biological, and chemical weapons programs. The analysts who worked Iraqi weapons issues universally agreed that in no instance did political pressure cause them to skew or alter any of their analytical judgments. That said, it is hard to deny the conclusion that intelligence analysts worked in an environment that did not encourage skepticism about the conventional wisdom.

Other Case Studies: An Overview

Our remaining case studies present a more mixed picture. On the positive side, Libya is fundamentally a success story. The Intelligence Community assessed correctly the state of Libya's nuclear and chemical weapons programs, and the Intelligence Community's use of new techniques to penetrate the A.Q. Khan network allowed the U.S. government to pressure Libya into dismantling those programs. In counterterrorism, the Intelligence Community has made great strides since September 11, in particular with respect to tactical operations overseas. These successes stemmed from isolated efforts that need to be replicated in other areas of intelligence; in the case of Libya, from innovative collection techniques and, in the case of terrorism, from an impressive fusion of interagency intelligence capabilities.

But we also reviewed the state of the Intelligence Community's knowledge about the unconventional weapons programs of several countries that pose current proliferation threats, including Iran, North Korea, China, and Russia. We cannot discuss many of our findings from these studies in our unclassified report, but we can say here that we found that we have only limited access to critical information about several of these high-priority intelligence targets.

Lessons Learned from the Case Studies

Our case studies revealed failures and successes that ran the gamut of the intelligence process. Although each of these studies is covered in far greater detail in the report itself, we include here a summary of the central lessons we drew from them.

Poor target development: not getting intelligence on the issues we care about most. You can't analyze intelligence that you don't have—and our case studies resoundingly demonstrate how little we know about some of our highest priority intelligence targets. It is clear that in today's context the traditional collection techniques employed by individual collection agencies have lost much of their power to surprise our adversaries. The successful penetrations of "hard targets" that we did find were usually the result either of an innovative collection technique or of a creative integration of collection capabilities across agencies. In general, however, the Intelligence Community has not developed the long-term, coordinated collection strategies that are necessary to penetrate today's intelligence targets.

Lack of rigorous analysis. Long after the Community's assessment of Iraq had begun to fall apart, one of the main drafters of the NIE told us that, if he had to grade it, he would still give the NIE an "A." By that, he presumably meant that the NIE fully met the standards for analysis that the Community had set for itself. That is the problem. The scope and quality of analysis has eroded badly in the Intelligence Community and it must be restored. In part, this is a matter of tradecraft and training; in part, too, it is a matter of expertise.

Analytic "tradecraft"—the way analysts think, research, evaluate evidence, write, and communicate—must be strengthened. In many instances, we found finished intelligence that was loosely reasoned, ill-supported, and poorly communicated. Perhaps most worrisome, we found too many analytic products that obscured how little the Intelligence Community actually *knew* about an issue and how much their conclusions rested on inference and assumptions. We believe these tendencies must be reversed if decisionmakers are to have confidence in the intelligence they receive. And equally important, analysts must be willing to admit what they don't know in order to focus future collection efforts. Conversely, policymakers must be prepared to accept

uncertainties and qualifications in intelligence judgments and not expect greater precision than the evaluated data permits.

Good "tradecraft" without expertise, however, will only get you so far. Our case studies identified areas in which the Community's level of expertise was far below what it should be. In several instances, the Iraq assessments rested on failures of technical analysis that should have been obvious at the time—failure to understand facts about weapons technology, for example, or failures to detect obvious forgeries. Technical expertise, particularly relating to weapons systems, has fallen sharply in the past ten years. And in other areas, such as biotechnology, the Intelligence Community is well behind the private sector.

But the problem of expertise goes well beyond technical knowledge. During the Cold War, the Intelligence Community built up an impressive body of expertise on Soviet society, organization, and ideology, as well as on the Soviet threat. Regrettably, no equivalent talent pool exists today for the study of Islamic extremism. In some cases, the security clearance process limits the Intelligence Community's ability to recruit analysts with contacts among relevant groups and with experience living overseas. Similarly, some security rules limit the ways in which analysts can develop substantive expertise. Finally, poor training or bad habits lead analysts to rely too much on secret information and to use non-clandestine and public information too little. Non-clandestine sources of information are critical to understanding societal, cultural, and political trends, but they are insufficiently utilized.

Lack of political context—and imagination. The October 2002 NIE contained an extensive technical analysis of Iraq's suspected weapons programs but little serious analysis of the socio-political situation in Iraq, or the motives and intentions of Iraqi leadership—which, in a dictatorship like Iraq, really meant understanding Saddam. It seems unlikely to us that weapons experts used to combing reports for tidbits on technical programs would ever have asked: "Is Saddam bluffing?" or "Could he have decided to suspend his weapons programs until sanctions are lifted?" But an analyst steeped in Iraq's politics and culture at least *might* have asked those questions, and, of course, those turn out to be the questions that could have led the Intelligence Community closer to the truth. In that respect, the analysts displayed a lack of imagination. The Iraq example also reflects the Intelligence Community's increasing tendency to separate regional, technical, and

(now) terrorism analysis—a trend that is being exacerbated by the gravitational pull toward centers like the National Counterterrorism Center (NCTC).

Overemphasis on and underperformance in daily intelligence products. As problematic as the October 2002 NIE was, it was not the Community's biggest analytic failure on Iraq. Even more misleading was the river of intelligence that flowed from the CIA to top policymakers over long periods of time—in the President's Daily Brief (PDB) and in its more widely distributed companion, the Senior Executive Intelligence Brief (SEIB). These daily reports were, if anything, more alarmist and less nuanced than the NIE. It was not that the intelligence was markedly different. Rather, it was that the PDBs and SEIBs, with their attention-grabbing headlines and drumbeat of repetition, left an impression of many corroborating reports where in fact there were very few sources. And in other instances, intelligence suggesting the existence of weapons programs was conveyed to senior policymakers, but later information casting doubt upon the validity of that intelligence was not. In ways both subtle and not so subtle, the daily reports seemed to be "selling" intelligence—in order to keep its customers, or at least the First Customer, interested.

Inadequate information sharing. There is little doubt that, at least in the context of counterterrorism, information sharing has improved substantially since September 11. This is in no small part due to the creation of the Terrorist Threat Integration Center (now NCTC) and the increased practice of housing collectors and analysts together, which provides a real-world solution to some of the bureaucratic and institutional barriers that exist between the big intelligence-collecting agencies. But in the three and a half years since September 11, this push to share information has not spread to other areas, including counterproliferation, where sharing is also badly needed. Furthermore, even in the counterterrorism context, information sharing still depends too much on physical co-location and personal relationships as opposed to integrated, Community-wide information networks. Equally problematic, individual departments and agencies continue to act as though they own the information they collect, forcing other agencies to pry information from them. Similarly, much information deemed "operational" by the CIA and FBI isn't routinely shared, even though analysts have repeatedly stressed its importance. All of this reveals that extensive work remains yet to be done.

Poor human intelligence. When the October 2002 NIE was written the United States had little human intelligence on Iraq's nuclear, biological, and chemical weapons programs and virtually no human intelligence on leadership intentions. While classification prevents us from getting into the details, the picture is much the same with respect to other dangerous threats. We recognize that espionage is always chancy at best; 50 years of pounding away at the Soviet Union resulted in only a handful of truly important human sources. Still, we have no choice but to do better. Old approaches to human intelligence alone are not the answer. Countries that threaten us are well aware of our human intelligence services' *modus operandi* and they know how to counter it. More of the same is unlikely to work. Innovation is needed. The CIA deserves credit for its efforts to discover and penetrate the A.Q. Khan network, and it needs to put more emphasis on other innovative human intelligence methods.

Worse than having no human sources is being seduced by a human source who is telling lies. In fact, the Community's position on Iraq's biological weapons program was largely determined by sources who were telling lies—most notably a source provided by a foreign intelligence service through the Defense Intelligence Agency. Why DIA and the rest of the Community didn't find out that the source was lying is a story of poor asset validation practices and the problems inherent in relying on semi-cooperative liaison services. That the NIE (and other reporting) didn't make clear to policymakers how heavily it relied on a single source that no American intelligence officer had ever met, and about whose reliability several intelligence professionals had expressed serious concern, is a damning comment on the Intelligence Community's practices.

The challenge to traditional signals intelligence. Signals intelligence—the interception of radio, telephone, and computer communications—has historically been a primary source of good intelligence. But changes in telecommunications technology have brought new challenges. This was the case in Iraq, where the Intelligence Community lost access to important aspects of Iraqi communications, and it remains the case elsewhere. We offer a brief additional discussion of some of the modern challenges facing signals intelligence in our classified report, but we cannot discuss this information in an unclassified format.

Regaining signals intelligence access must be a top priority. The collection agencies are working hard to restore some of the access that they have lost; and they've had some successes. And again, many of these recent steps in the right direction are the result of innovative examples of cross-agency cooperation. In addition, successful signals intelligence will require a sustained research and development effort to bring cutting-edge technology to operators and analysts. Success on this front will require greater willingness to accept financial costs, political risks, and even human casualties.

Declining utility of traditional imagery intelligence against unconventional weapons programs. The imagery collection systems that were designed largely to work against the Soviet Union's military didn't work very well against Iraq's unconventional weapons program, and our review found that they aren't working very well against other priority targets, either. That's because our adversaries are getting better at denial and deception, and because the threat is changing. Again, we offer details about the challenges to imagery intelligence in our classified report that we cannot provide here.

Making the problem even more difficult, there is little that traditional imagery can tell us about chemical and biological facilities. Biological and chemical weapons programs for the most part can exist inside commercial buildings with no suspicious signatures. This means that we can get piles of incredibly sharp photos of an adversary's chemical factories, and we still will not know much about its chemical weapons programs. We can still see a lot—and imagery intelligence remains valuable in many contexts, including support to military operations and when used in conjunction with other collection disciplines—but too often what we can see doesn't tell us what we need to know about nuclear, biological, and chemical weapons.

Measurement and signature intelligence (MASINT) is not sufficiently developed. The collection of technologies known as MASINT, which includes a virtual grab bag of advanced collection and analytic methods, is not yet making a significant contribution to our intelligence efforts. In Iraq, MASINT played a negligible role. As in other contexts, we believe that the Intelligence Community should continue to pursue new technology aggressively—whether it is called MASINT, imagery, or signals intelligence. Innovation will be necessary to defeat our adversaries' denial and deception.

An absence of strong leadership. For over a year, despite unambiguous presidential direction, a turf battle raged between CIA's Counterterrorist Center (CTC) and the Terrorist Threat Integration Center (now NCTC). The two organizations fought over roles, responsibilities, and resources, and the Intelligence Community's leadership was unable to solve the problem. The intelligence reform act may put an end to this particular conflict, but we believe that the story reflects a larger, more pervasive problem within the Intelligence Community: the difficulty of making a decision and imposing the consequences on all agencies throughout the Community. Time and time again we have uncovered instances like this, where powerful agencies fight to a debilitating stalemate masked as consensus, because no one in the Community has been able to make a decision and then make it stick. The best hope for filling this gap is an empowered DNI.

LOOKING FORWARD: OUR RECOMMENDATIONS FOR CHANGE

Our case studies collectively paint a picture of an Intelligence Community with serious deficiencies that span the intelligence process. Stated succinctly, it has too little *integration* and too little *innovation* to succeed in the 21st century. It rarely adopts integrated strategies for penetrating high-priority targets; decisionmakers lack authority to resolve agency disputes; and it develops too few innovative ways of gathering intelligence.

This section summarizes our major recommendations on how to change this state of affairs so that full value can be derived from the many bright, dedicated, and deeply committed professionals within the Intelligence Community. We begin at the top, and suggest how to use the opportunity presented by the new intelligence reform legislation to bring better integration and management to the Intelligence Community. Our management recommendations are developed in greater detail in Chapter Six of our report. We next offer recommendations that would improve intelligence collection (Chapter 7) and analysis (Chapter 8). Then we examine several specific and important intelligence challenges—improving information sharing (Chapter 9); integrating domestic and foreign intelligence in a way that both satisfies national security imperatives and safeguards civil liberties (Chapter 10); organizing the Community's counterintelligence mission (Chapter 11); and a largely classified chapter on managing covert action (Chapter 12). We then devote a stand-alone chapter to

examining the most dangerous unconventional weapons challenges the Intelligence Community faces today and offer specific prescriptions for improving our intelligence capabilities against these threats (Chapter 13).

Leadership and Management: Forging an Integrated Intelligence Community

A former senior Defense Department official described today's Intelligence Community as "not so much poorly managed as unmanaged." We agree. Everywhere we looked, we found important (and obvious) issues of interagency coordination that went unattended, sensible Community-wide proposals blocked by pockets of resistance, and critical disputes left to fester. Strong interagency cooperation was more likely to result from bilateral "treaties" between big agencies than from Community-level management. This ground was well-plowed by the 9/11 Commission and by several other important assessments of the Intelligence Community over the past decade.

In the chapter of our report devoted to management (Chapter 6), we offer detailed recommendations that we believe will equip the new Director of National Intelligence to forge today's loose confederation of 15 separate intelligence operations into a real, integrated Intelligence Community. A short summary of our more important management recommendations follows:

- ***Strong leadership and management of the Intelligence Community are indispensable.*** Virtually every senior intelligence official acknowledged the difficulty of leading and managing the Intelligence Community. Along with acting as the President's principal intelligence advisor, this will be the DNI's main job. His success in that job will determine the fate of many other necessary reforms. We thus recommend ways in which the DNI can use his limited, but not insignificant, authorities over money and people. No matter what, the DNI will not be able to run the Intelligence Community alone. He will need to create a management structure that allows him to see deep into the Intelligence Community's component agencies, and he will need to work closely with the other cabinet secretaries—especially the Secretary of Defense—for whom several Intelligence Community agencies also work. New procedures are particularly needed in the budget area, where today's Intelligence Community has a wholly inadequate Planning, Programming, and Budgeting System.

- ***Organize around missions.*** One of the most significant problems we identified in today's Intelligence Community is a lack of cross-Community focus on priority intelligence missions. By this, we mean that in most cases there is not one office, or one individual, who is responsible for making sure the Intelligence Community is doing all it can to collect and analyze intelligence on a subject like proliferation, or a country like Iran. Instead, intelligence agencies allocate their scarce resources among intelligence priorities in ways that seem sensible to them but are not optimal from a Community-wide perspective. The DNI needs management structures and processes that ensure a strategic, Community-level focus on priority intelligence missions. The specific device we propose is the creation of several "Mission Managers" on the DNI staff who are responsible for developing strategies for all aspects of intelligence relating to a priority intelligence target: the Mission Manager for China, for instance, would be responsible for driving collection on the China target, watching over China analysis, and serving as a clearinghouse for senior policymakers seeking China expertise.

- ***Establish a National Counter Proliferation Center.*** The new intelligence legislation creates one "national center"—the National Counterterrorism Center (NCTC)—and suggests the creation of a second, similar center devoted to counterproliferation issues. We agree that a National Counter Proliferation Center (NCPC) should be established but believe that it should be fundamentally different in character from the NCTC. The NCTC is practically a separate agency; its large staff is responsible not only for conducting counterterrorism analysis and intelligence gathering but also for "strategic operational planning" in support of counterterrorism policy. In contrast, we believe that the NCPC should be a relatively small center (*i.e.*, fewer than 100 people); it should primarily play a *management and coordination* function by overseeing analysis and collection on nuclear, biological, and chemical weapons across the Intelligence Community. In addition, although we agree that government-wide strategic planning is required to confront proliferation threats, we believe that entities other than the NCPC—such as a Joint Interagency Task Force we propose to coordinate interdiction efforts—should perform this function.

- ***Build a modern workforce.*** The intelligence reform legislation grants the DNI substantial personnel authorities. In our view, these authorities

come none too soon. The Intelligence Community has difficulty recruiting and retaining individuals with critically important skill sets—such as technical and scientific expertise, and facility with foreign languages—and has not adapted well to the diverse cultures and settings in which today's intelligence experts must operate. We propose the creation of a new human resources authority in the Office of the DNI to develop Community-wide personnel policies and overcome these systemic shortcomings. We also offer specific proposals aimed at encouraging "joint" assignments between intelligence agencies, improving job training at all stages of an intelligence professional's career, and building a better personnel incentive structure.

- ***Create mechanisms for sustained oversight from outside the Intelligence Community—and for self-examination from the inside.*** Many sound past proposals for intelligence reform have withered on the vine. Either the Intelligence Community is inherently resistant to outside recommendations, or it lacks the institutional capacity to implement them. In either case, sustained external oversight is necessary. We recommend using the new Joint Intelligence Community Council—which comprises the DNI and the cabinet secretaries with intelligence responsibilities—as a high-level "consumer council." We also recommend the President's Foreign Intelligence Advisory Board play a more substantial advisory role. Like others before us, we suggest that the President urge Congress to reform its own procedures to provide better oversight. In particular, we recommend that the House and Senate intelligence committees create focused oversight subcommittees, that the Congress create an intelligence appropriations subcommittee and reduce the Intelligence Community's reliance on supplemental funding, and that the Senate intelligence committee be given the same authority over joint military intelligence programs and tactical intelligence programs that the House intelligence committee now exercises. Finally—and perhaps most importantly—we recommend that the DNI create mechanisms to ensure that the Intelligence Community conducts "lessons learned" and after-action studies so that it will be better equipped to identify its *own* strengths and weaknesses.

Additional Leadership and Management Recommendations

In addition to those described above, Chapter Six of our report offers recommendations concerning:

- How to build a coordinated process for "target development"—that is, the directing of collection resources toward priority intelligence subjects;
- How to spur innovation outside individual collection agencies;
- How the DNI might handle the difficult challenges of integrating intelligence from at home and abroad, and of coordinating activities and procedures with the Department of Defense; and
- How the DNI might organize the office of the DNI to fit needed leadership and management functions into the framework created by the intelligence reform legislation.

Integrated and Innovative Collection

The intelligence failure in Iraq did not begin with faulty analysis. It began with a sweeping collection failure. The Intelligence Community simply couldn't collect good information about Iraq's nuclear, biological, or chemical programs. Regrettably, the same can be said today about other important targets, none of which will ever be easy targets—but we can and should do better.

Urging each individual collection agency to do a better job is not the answer. Where progress has been made against such targets, the key has usually been more integration and more innovation in collecting intelligence. As a result, we recommend the following:

- ***Create a new Intelligence Community process for managing collection as an "integrated enterprise."*** In order to gather intelligence effectively, the Intelligence Community must develop and buy sophisticated technical collection systems, create strategies for focusing those systems on priority targets, process and exploit the data that these systems collect, and plan for the acquisition of future systems. Today, each of these functions is performed primarily within individual collection agencies, often with little or no Community-level direction or interagency coordination. We propose that the DNI create what we call an

"integrated collection enterprise" for the Intelligence Community—that is, a management structure in which the Community's decentralized collection capabilities are harmonized with intelligence priorities and deployed in a coordinated way.

- ***Create a new Human Intelligence Directorate.*** Both the Defense Department and the FBI are substantially increasing their human intelligence activities abroad, which heightens the risk that intelligence operations will not be properly coordinated with the CIA's human espionage operations, run by its Directorate of Operations (DO). The human intelligence activities of the Defense Department and the FBI should continue, but in the world of foreign espionage, a lack of coordination can have dangerous, even fatal, consequences. To address this pressing problem, we suggest the creation of a new Human Intelligence Directorate within the CIA, to which the present DO would be subordinate, to ensure the coordination of all U.S. agencies conducting human intelligence operations overseas. In addition to this coordination role, the Human Intelligence Directorate would serve as the focal point for Community-wide human intelligence issues, including helping to develop a national human intelligence strategy, broadening the scope of human intelligence activities, integrating (where appropriate) collection and reporting systems, and establishing Community-wide standards for training and tradecraft.

- ***Develop innovative human intelligence techniques.*** The CIA's Directorate of Operations is one of the Intelligence Community's elite and storied organizations. However, the DO has remained largely wedded to the traditional model—a model that does not meet the challenges posed by terrorist organizations and nations that are "denied areas" for U.S. personnel. Accordingly, we recommend the establishment of an "Innovation Center" within the CIA's new Human Intelligence Directorate—but *not* within the DO. This center would spur the use of new and nontraditional methods of collecting human intelligence. In the collection chapter of our report, we also detail several new methods for collecting human intelligence that in our judgment should either be explored or used more extensively.

- ***Create an Open Source Directorate within the CIA.*** We are convinced that analysts who use open source information can be more effective

than those who don't. Regrettably, however, the Intelligence Community does not have an entity that collects, processes, and makes available to analysts the mass of open source information that is available in the world today. We therefore recommend the creation of an Open Source Directorate at the CIA. The directorate's mission would be to deploy sophisticated information technology to make open source information available across the Community. This would, at a minimum, mean gathering and storing digital newspapers and periodicals that are available only temporarily on the Internet and giving Intelligence Community staff easy (and secure) access to Internet materials. In addition, because we believe that part of the problem is analyst resistance, not lack of collection, we recommend that some of the new analysts allocated to CIA be specially trained to use open sources and then to act as open source "evange-analysts" who can jumpstart the open source initiative by showing its value in addressing particular analytic problems. All of this, we believe, will help improve the Intelligence Community's surprisingly poor "feel" for cultural and political issues in the countries that concern policymakers most. The Open Source Directorate should also be the primary test bed for new information technology because the security constraints—while substantial—are lower for open source than for classified material.

- ***Reconsider MASINT.*** Measurements and signatures can offer important intelligence about nuclear, biological, and chemical weapons. But the tools we use to collect these measurements and signatures—tools collectively referred to within the intelligence community as "MASINT"—do not obviously constitute a single discipline. In a world of specialized collection agencies, there is reason to suspect that these orphaned technologies may have been under-funded and under-utilized. We recommend that the DNI take responsibility for developing and coordinating new intelligence technologies, including those that now go under the title MASINT. This could be done by a special coordinator, or as part of the DNI's Office of Science and Technology. The DNI's office does not need to directly control MASINT collection. Rather, we recommend that individual collection agencies assume responsibility for aspects of MASINT that fall naturally into their bailiwicks. At the same time, the DNI's designated representative would promote and monitor the status of new technical intelligence programs throughout the Intelligence

Community to ensure that they are fully implemented and given the necessary attention.

Additional Collection Recommendations

In addition to those described above, Chapter Seven of our report offers recommendations concerning:

- Developing new human and technical collection methods;
- Professionalizing human intelligence across the Intelligence Community;
- Creating a larger and better-trained human intelligence officer cadre;
- Amending the Foreign Intelligence Surveillance Act to extend the duration of certain forms of electronic surveillance against non-U.S. persons, to ease administrative burdens on NSA and the Department of Justice; and
- Improving the protection of sources and methods by reducing authorized and unauthorized disclosures.

Transforming Analysis

Integrated, innovative collection is just the beginning of what the Intelligence Community needs. Some of the reforms already discussed, particularly the DNI-level "Mission Managers," will improve analysis. But much more is needed. In particular, analytic expertise must be deepened, intelligence gaps reduced, and existing information made more usable—all of which would improve the quality of intelligence.

As an overarching point, however, the Intelligence Community must recognize the central role of analysts in the intelligence process. Needless to say, analysts are the people who analyze intelligence, put it in context, and communicate the intelligence to the people who need it. But in addition, analysts are the repositories for what the Intelligence Community *doesn't* know, and they must clearly convey these gaps to decisionmakers—as well as to collectors so that the Intelligence Community does everything it can to fill the holes. (Analysts will also play an increasingly prominent role in information security, as they "translate" intelligence from the most sensitive of sources to a variety of consumers, ranging from state and local first responders to senior policymakers.) To enable analysts to fulfill these roles, we recommend the following:

- ***Empower Mission Managers to coordinate analytic efforts on a given topic.*** The Mission Managers we propose would serve as the focal point for all aspects of the intelligence effort on a particular issue. They would be aware of the analytic expertise in various intelligence agencies, assess the quality of analytic products, identify strategic questions receiving inadequate attention, encourage alternative analysis, and ensure that dissenting views are expressed to intelligence users. When necessary, they would recommend that the DNI use his personnel authorities to move analysts to priority intelligence topics. At the same time, Mission Managers should *not* be responsible for providing a single, homogenized analytic product to decisionmakers; rather, Mission Managers should be responsible for encouraging alternative analysis and for ensuring that dissenting views are expressed to intelligence customers. In sum, Mission Managers should be able to find the right people and expertise and make sure that the right analysis, including alternative analysis, is getting done.

- ***Strengthen long-term and strategic analysis.*** The most common complaint we heard from analysts in the Intelligence Community was that the pressing demand for current intelligence "eats up everything else." Analysts cannot maintain their expertise if they cannot conduct long-term and strategic analysis. Because this malady is so pervasive and has proven so resistant to conventional solutions, we recommend establishing an organization to perform only long-term and strategic analysis under the National Intelligence Council, the Community's existing focal point for interagency long-term analytic efforts. The new unit could serve as a focal point for Community-wide alternative analysis, thereby complementing agency-specific efforts at independent analysis. And although some analysts in this organization would be permanently assigned, at least half would serve only temporarily and would come from all intelligence agencies, including NGA and NSA, as well as from outside the government. Such rotations would reinforce good tradecraft habits, as well as foster a greater sense of Community among analysts and spur collaboration on other projects.

- ***Encourage diverse and independent analysis.*** We believe that diverse and independent analysis—often referred to as "competitive analysis"—should come from many sources. As we have just noted, we recommend that our proposed long-term research and analysis unit, as well

as the National Intelligence Council, conduct extensive independent analysis. In some circumstances there is also a place for a "devil's advocate"—someone appointed to challenge the consensus view. We also think it important that a not-for-profit "sponsored research institute" be created *outside* the Intelligence Community; such an institute would serve as a critical window into outside expertise, conduct its own research, and reach out to specialists, including academics and technical experts, business and industry leaders, and representatives from the nonprofit sector. Finally, the Intelligence Community should encourage independent analysis throughout its analytic ranks. In our view, this can best be accomplished through the preservation of dispersed analytic resources (as opposed to consolidation in large "centers"), active efforts by Mission Managers to promote independent analysis, and Community-wide training that instills the importance of such analysis.

- ***Improve the rigor and "tradecraft" of analysis.*** Our studies, and many observers, point to a decline in analytic rigor within the Intelligence Community. Analysts have suffered from weak leadership, insufficient training, and budget cutbacks that led to the loss of our best, most senior analysts. There is no quick fix for tradecraft problems. However, we recommend several steps: increasing analyst training; ensuring that managers and budget-writers allot time and resources for analysts to actually *get* trained; standardizing good tradecraft practices through the use of a National Intelligence University; creating structures and practices that increase competitive analysis; increasing managerial training for Intelligence Community supervisors; enabling joint and rotational assignment opportunities; ensuring that finished intelligence products are sufficiently transparent so that an analyst's reasoning is visible to intelligence customers; and implementing other changes in human resource policies—such as merit-based-pay—so that the best analysts are encouraged to stay in government service.

- ***Communicating intelligence to policymakers.*** The best intelligence in the world is worthless unless it is effectively and accurately communicated to those who need it. The Iraq weapons of mass destruction case is a stark example. The daily reports sent to the President and senior policymakers discussing Iraq over many months proved to be disastrously one-sided. We thus offer recommendations on ways in which intelligence products can be enhanced, including how the President's Daily

Brief (PDB) might be improved. In this regard, we suggest the elimination of the inherently misleading "headline" summaries in PDBs and other senior policymaker briefs, and that the DNI oversee production of the PDB. To accomplish this, we recommend the DNI create an analytic staff too small to routinely undertake drafting itself, but large enough to have background on many of the issues that are covered by the PDB. The goal would be to enable the DNI to coordinate and oversee the process, without requiring him to take on the heavy—and almost overwhelming—mantle of daily intelligence support to the President. Critically, the DNI's staff would also ensure that the PDB reflects alternative views from the Community to the greatest extent feasible.

We also recommend that the DNI take responsibility, with the President's concurrence, for the three primary sources of intelligence that now reach the President: the PDB, the President's Terrorism Threat Report—a companion publication produced by the NCTC and focused solely on terrorism-related issues—and the briefing by the Director of the FBI. We suggest that the DNI coordinate this intelligence in a manner that eliminates redundancies and ensures that only material that is necessary for the President be included. We think this last point is especially important because we have observed a disturbing trend whereby intelligence is passed to the President (as well as other senior policymakers) not because it requires high-level attention, but because passing the information "up the chain" provides individuals and organizations with bureaucratic cover.

- ***Demand more from analysts.*** We urge that policymakers actively probe and question analysts. In our view, such interaction is not "politicization." Analysts should expect such demanding and aggressive testing without—as a matter of principle and professionalism—allowing it to subvert their judgment.

Additional Analysis Recommendations

In addition to those described above, Chapter Eight of our report offers recommendations concerning:

- Developing technologies capable of exploiting large volumes of foreign language data without the need for human translations;

Additional Analysis Recommendations (Continued)

- Improving career-long analytical and managerial training;
- Creating a database for all finished intelligence, as well as adopting technology to update analysts and decisionmakers when intelligence judgments change;
- Improving the Intelligence Community's science, technology, and weapons expertise;
- Changing the way analysts are hired, promoted, and rewarded; and
- Institutionalizing "lessons learned" procedures to learn from past analytical successes and failures.

Information Sharing

While the new intelligence reform legislation correctly identifies information sharing as an area where major reforms are necessary, the steps it takes to address the problem raise as many questions as they answer. The legislation creates a new position—a "Program Manager" who sits outside of the Intelligence Community and reports directly to the President—responsible for creating an integrated, government-wide Information Sharing Environment for all "terrorism information." At the same time, the Director of National Intelligence is given responsibility for facilitating information sharing for *all* intelligence information *within* the Intelligence Community.

We believe that these two separate statutory information sharing efforts should be harmonized. We are less confident that any particular mechanism is optimal. Perhaps the least bad solution to this tricky problem—short of new legislation—is to require that the Program Manager report to the President *through* the DNI, and that the Information Sharing Environment be expanded to include all intelligence information, not just intelligence related to terrorism. In recommending this solution, however, we emphasize that information sharing cannot be understood merely as an Intelligence Community endeavor; whoever leads the effort to build the Information Sharing Environment must be sensitive to the importance of distributing necessary information to those who need it both in the non-intelligence components of the federal government, and to relevant state, local, and tribal authorities.

We also make specific recommendations concerning how best to implement the information sharing effort. Among these recommendations are: designating a single official under the DNI who will be responsible for both information sharing *and* information security, in order to break down cultural and policy barriers that have impeded the development of a shared information space; applying advanced technologies to the Information Sharing Environment to permit more expansive sharing with far greater security protections than currently exist in the Intelligence Community; and establishing clear and consistent Community-wide information sharing and security policies. Last but not least, we recommend that the DNI jettison the phrase "information sharing" itself, which merely reinforces the (incorrect) notion that information is the property of individual intelligence agencies, rather than of the government as a whole.

Finally, we believe it is essential to note the importance of protecting civil liberties in the context of information sharing. We believe that the intelligence reform act provides the framework for appropriate protection of civil liberties in this area, and that all information sharing must be done in accordance with Attorney General guidelines relating to "U.S. persons" information. At the same time, in our view the pursuit of privacy and national security is *not* a zero-sum game. In fact, as we describe in our report, many of the very same tools that provide counterintelligence protection can be equally valuable in protecting privacy.

Intelligence at Home: the FBI, Justice, and Homeland Security

Although the FBI has made strides in turning itself into a true collector and analyst of intelligence, it still has a long way to go. The Bureau, among other things, has set up Field Intelligence Groups in each of its 56 field offices and created an Executive Assistant Director for Intelligence with broad responsibility for the FBI's intelligence mission. Yet even FBI officials acknowledge that its collection and analysis capabilities will be a work in progress until at least 2010.

In our view, the biggest challenge is to make the FBI a full participant in the Intelligence Community. This is not just a matter of giving the Bureau new resources and new authority. It must also mean integrating the FBI into a Community that is subject to the DNI's coordination and leadership. Unfortunately, the intelligence reform legislation leaves the FBI's relationship to the

DNI especially murky. We recommend that the President make clear that the FBI's intelligence activities are to be fully coordinated with the DNI and the rest of the Community.

- ***Create a separate National Security Service within the FBI that includes the Bureau's Counterintelligence and Counterterrorism Divisions, as well as the Directorate of Intelligence.*** The intelligence reform act empowers the DNI to lead the Intelligence Community, which includes the FBI's "intelligence elements." Although the statute leaves the term ambiguous, we believe that "elements" must include *all* of the Bureau's national security-related components—the Intelligence Directorate *and* the Counterterrorism and Counterintelligence Divisions. Anything less and the DNI's ability to coordinate intelligence across our nation's borders will be dangerously inadequate.

  Simply granting the DNI authority over the Bureau's current Directorate of Intelligence is, we believe, insufficient. We say this because the Directorate of Intelligence has surprisingly little operational, personnel, and budgetary authority. Currently the directorate has no authority to initiate, terminate, or re-direct any collection or investigative operation in any of the FBI's 56 regional field offices that are scattered throughout the nation or within any of the four operational divisions (Counterintelligence, Counterterrorism, Cyber, and Criminal) at FBI Headquarters. Although the Directorate of Intelligence may "task" the field offices to collect against certain requirements, it has no direct authority to ensure that FBI resources actually carry out these requirements. Its "taskings" are really "askings." Nor does the directorate contain the great bulk of the FBI's intelligence analysts. And the directorate has no clear control over the Bureau's portion of the National Intelligence Program budget, which is largely spent by the Counterterrorism and Counterintelligence Divisions. In short, the intelligence directorate has few, if any, mechanisms for exercising direct authorities over FBI's intelligence collectors or analytic products. With a direct line of authority only to the Bureau's Directorate of Intelligence, the DNI cannot be ensured influence over the Bureau's national security functions, and the FBI will not be fully integrated into the Intelligence Community.

  We therefore recommend the creation of a separate National Security Service *within the FBI* that has full authority to manage, direct, and control

all Headquarters and Field Office resources engaged in counterintelligence, counterterrorism, and foreign intelligence collection, investigations, operations, and analysis. Critically, this division would then be subject to the same DNI authorities as apply to such Defense agencies as NSA and NGA. Of equal importance, this structure would maintain the Attorney General's oversight of the FBI's activities to ensure the Bureau's compliance with U.S. law. In this sense, the Attorney General's role would be similar to that of the Secretary of Defense, who—even with the appointment of the DNI—continues to oversee Defense Department agencies within the Intelligence Community, like NSA and NGA.

- ***Ensure better mechanisms for coordination and cooperation on foreign intelligence collection in the United States.*** The expansion of the FBI's intelligence collection and reporting activities over the past few years has engendered turf battles between the CIA and the FBI that have already caused counterproductive conflicts both within and outside of the United States. In particular, the two agencies have clashed over the domestic collection of foreign intelligence—an area in which they have long shared responsibilities. We see no reason to change the status quo dramatically or to expand the FBI's authority over foreign intelligence gathering inside the United States. If unanticipated conflicts emerge, both agencies should be instructed to take their differences to the DNI for resolution. The two agencies' capabilities should complement, rather than compete with, one another. We also expect that such an integrated approach would continue to rely on the existing Attorney General guidelines, which carefully limit the way both agencies operate within the United States, and with regard to U.S. persons overseas. We believe that strong CIA/FBI cooperation and clear guidelines are essential for protection of civil liberties as well as for effective intelligence gathering.

- ***Reorient the Department of Justice.*** Every agency that has major responsibility for terrorism and intelligence has been overhauled in the past four years. With one exception: at the Department of Justice, the famous "wall" between intelligence and criminal law still lingers, at least on the organization charts. On one side is the Office of Intelligence Policy and Review, which handles Foreign Intelligence Surveillance Court orders—those court orders that permit wiretaps and physical searches for national security reasons. On the other side are two separate sections of the Criminal Division (Counterterrorism and Counterespionage), reporting to two separate Deputy

Assistant Attorneys General. This organizational throwback to the 1990s scatters intelligence expertise throughout the Department and in some cases has contributed to errors that hampered intelligence gathering. A single office with responsibility for counterterrorism, counterintelligence, and intelligence investigations would ensure better communication and reduce the tendency to rebuild the wall along bureaucratic lines.

We recommend that these three components (perhaps joined by a fourth Justice Department component that coordinates issues related to transnational crimes) be placed together under the authority of an Assistant Attorney General for National Security who would, like the Assistant Attorney General for the Criminal Division, report either directly to the Deputy Attorney General, or to a newly created Associate Attorney General responsible for both the National Security and Criminal Divisions.

- ***Strengthen the Department of Homeland Security's relationship with the Intelligence Community.*** The Department of Homeland Security is the primary repository of information about what passes in and out of the country—a critical participant in safeguarding the United States from nuclear, biological, or chemical attack. Yet, since its inception, Homeland Security has faced immense challenges in collecting information effectively, making it available to analysts and users both inside and outside the Department, and bringing intelligence support to law enforcement and first responders who seek to act on such information. We did not conduct a detailed study of Homeland Security's capabilities, but it is clear to us that the department faces challenges in all four roles it plays in the intelligence community—as collector, analyst, disseminator, and customer.

  Among the obstacles confronting Homeland Security, we found during the course of our study that the Department's Immigration and Customs Enforcement still operates under an order inherited from the Treasury Department in the 1980s. The order requires high-level approval for virtually all information sharing and assistance to the Intelligence Community. We think this order should be rescinded, and we believe the DNI should carefully examine how Homeland Security works with the rest of the Intelligence Community.

Counterintelligence

Every intelligence service on the planet wants to steal secrets from the last remaining superpower. But as other nations increase their intelligence operations against the United States, U.S. counterintelligence has been in a defensive crouch—fractured, narrowly focused, and lacking national direction. This may change as a result of the President's newly announced counterintelligence strategy. The good ideas in the strategy must, however, still be put into practice.

CIA does counterintelligence abroad, but its capabilities are limited. The FBI's counterintelligence efforts within the United States are well-staffed, but hardly strategic in their nature. Finally, the Defense Department's counterintelligence capabilities lack effective cross-department integration and direction. To address these concerns, we recommend four steps to strengthen counterintelligence: the empowerment of the nation's chief counterintelligence officer, the National Counterintelligence Executive (NCIX); the development of a new CIA capability for enhancing counterintelligence abroad; the centralization of the Defense Department's counterintelligence functions; and, as suggested earlier, bringing the FBI into the Intelligence Community to ensure that its robust counterintelligence capabilities are employed in line with the DNI's priorities. Moreover, all of these efforts must focus greater attention on the technical aspects of counterintelligence, as our adversaries shift from human spying to attempting to penetrate our information infrastructure.

Covert Action

If used in a careful and limited way, covert action can serve as a more subtle and surgical tool than forms of acknowledged employment of U.S. power and influence. As part of our overall review of the Intelligence Community, we conducted a careful study of U.S. covert action capabilities. Our findings were included in a short, separate chapter of our classified report. Regrettably, this area is so heavily classified that we could not include a chapter on the subject in our unclassified report.

We will, however, state here—at a necessarily high level of generality—some of our overall conclusions on covert action. At the outset, we note that we found current covert action programs in the counterproliferation and counterterrorism areas to be energetic, innovative, and well-executed within

the limits of their authority and funding. Yet some critically important programs are hobbled by lack of sustained strategic planning, insufficient commitment of resources on a long-term basis, and a disjointed management structure. In our classified report we suggest organizational changes that we believe would consolidate support functions for covert action and improve the management of covert action programs within the Intelligence Community; we are unable to provide further details on these recommendations, however, in this unclassified format.

Addressing Proliferation

So far, we have focused on improving the Intelligence Community writ large—on the theory that only a redesigned Community can substantially improve its performance in assessing the threat posed by weapons of mass destruction. But quite apart from the structural changes we have already recommended, the Intelligence Community also needs to change the way it approaches two of the greatest threats—biological weapons and new forms of nuclear proliferation.

Biological Weapons

The 2001 anthrax attacks on the United States killed five people, crippled mail delivery in several cities for a year, and imposed more than a billion dollars in decontamination costs. For all that, we were lucky. Biological weapons are cheaper and easier to acquire than nuclear weapons—and they could be more deadly. The threat is deeply troubling today; it will be more so tomorrow, when genetic modification techniques will allow the creation of even worse biological weapons. Most of the traditional Intelligence Community collection tools are of little or no use in tackling biological weapons. In our classified report, we discuss some of the specific challenges that confront our intelligence effort against the biological threat—but regrettably we cannot discuss them here.

Faced with a high-priority problem that does not yield to traditional methods, large parts of the Intelligence Community seem to have lowered their expectations and focused on other priorities. This is unacceptable. The Intelligence Community, and the government as a whole, needs to approach the problem with a new urgency and new strategies:

- ***Work with the biological sciences community.*** The Intelligence Community simply does not have the in-depth technical knowledge about biological weapons that it has about nuclear weapons. To close the expertise gap, the Community cannot rely on hiring biologists, whose knowledge and skills are extremely important, but whose depth and timeliness of expertise begins eroding as soon as they move from the laboratory to the intelligence profession. Instead, the DNI should create a Community Biodefense Initiative to institutionalize outreach to technical experts inside and outside of government. We describe specific components of this initiative in the body of our report.

- ***Make targeted collection of biological weapons intelligence a priority within the Intelligence Community.*** The Intelligence Community's collection woes starkly illustrate the need for more aggressive, targeted approaches to collection on biological threats. We recommend that the DNI create a deputy within the National Counter Proliferation Center who is specifically responsible for biological weapons; this deputy would ensure the implementation of a comprehensive biological weapons targeting strategy, which would entail gaining real-time access to non-traditional sources of information, filtering open source data, and devising specific collection initiatives directed at the resulting targets.

- ***Leverage regulation for biological weapons intelligence.*** The United States should look outside of intelligence channels for enforcement mechanisms that can provide new avenues of international cooperation and resulting opportunities for intelligence collection on biological threats. In the corresponding chapter of our report, we recommend encouraging foreign criminalization of biological weapons development and establishing biosafety and biosecurity regulations under United Nations Security Council Resolution 1540. We also propose extending biosecurity and biosafety regulations to foreign institutions with commercial ties to the United States.

Nuclear Weapons

The intelligence challenge posed by nuclear weapons continues to evolve. The Intelligence Community must continue to monitor established nuclear states such as Russia and China, and at the same time face newer and potentially more daunting challenges like terrorist use of a nuclear weapon. But the focus of the U.S. Intelligence Community has historically been on the capa-

bilities of large nation states. When applied to the problem of terrorist organizations and smaller states, many of our intelligence capabilities are inadequate.

The challenges posed by the new environment are well-illustrated by two aspects of nuclear proliferation. The first is the continuing challenge of monitoring insecure nuclear weapons and materials, or "loose nukes"—mainly in the former Soviet Union but also potentially in other nations. The second aspect is the appearance of non-state nuclear "brokers," such as the private proliferation network run by the Pakistani scientist A.Q. Khan. In Khan's case, innovative human intelligence efforts gave the United States access to this proliferation web. However, not only does the full scope of Khan's work remain unknown, but senior officials readily acknowledge that the Intelligence Community must know more about the private networks that support proliferation. The Intelligence Community must adapt to the changing threat.

Intelligence Support to Interdiction

So far, the Intelligence Community has enjoyed a number of successes intercepting materials related to nuclear, biological, and chemical weapons (and their related delivery systems)—the process commonly referred to as "interdiction." But success has come at a cost. The Intelligence Community has focused so much energy on its own efforts that the Community shows less ambition and imagination in supporting other agencies that should play a large role in interdiction. Many other federal agencies could do more to interdict precursors, weapons components, and dangerous agents if they had effective intelligence support. We recommend several mechanisms to improve intelligence support to these agencies, most particularly the creation of a counterproliferation Joint Interagency Task Force modeled on similar entities that have proved successful in the counternarcotics context.

Moreover, since it may not be possible in all cases to identify proliferation shipments before they reach the United States, our last line of defense is detecting and stopping these shipments before they reach our border. Yet new sensor technologies have faced challenges. In the corresponding chapter of this report, we suggest how the Intelligence Community and Department of Homeland Security can work together on this issue.

Leveraging Legal and Regulatory Mechanisms

Intelligence alone cannot solve the proliferation threat. But it may not have to. Information that spies and eavesdroppers would spend millions for and risk their lives to steal can sometimes be easily obtained by the right Customs, Treasury, or export control officials. The industries that support proliferation are subject to a host of regulatory regimes. But the agencies that regulate industry in these areas—Treasury, State, Homeland Security, and Commerce—do not think of themselves as engaged in the collection of intelligence, and the Intelligence Community only rarely appreciates the authorities and opportunities presented by regulatory regimes.

Given the challenges presented by quasi-governmental proliferation, the United States must leverage all of its capabilities to flag potential proliferators, gain insight into their activities, and interdict them, where appropriate. We therefore recommend a series of possible changes to existing regulatory regimes, all designed to improve insight into nuclear, biological, or chemical proliferation and enhance our ability to take action. These changes include negotiating ship boarding agreements that include tagging and tracking provisions to facilitate the surveillance of suspect vessels, taking steps to facilitate greater coordination between the Commerce Department (and Immigrations and Customs Enforcement) and the Intelligence Community, using Commerce Department and Customs and Border Protection regulations to facilitate information sharing about suspect cargo and persons and to justify related interdictions, and expanding the Treasury Department's authority to block assets of proliferators.

CONCLUSION

The harm done to American credibility by our all too public intelligence failings in Iraq will take years to undo. If there is good news it is this: without actually suffering a massive nuclear or biological attack, we have learned how badly the Intelligence Community can fail in struggling to understand the most important threats we face. We must use the lessons from those failings, and from our successes as well, to improve our intelligence for the future, and do so with a sense of urgency. We already have thousands of dedicated officers and many of the tools needed to do the job. With that in mind, we now turn first to what went wrong in Iraq, then to other intelligence cases, and finally to our detailed recommendations for action.