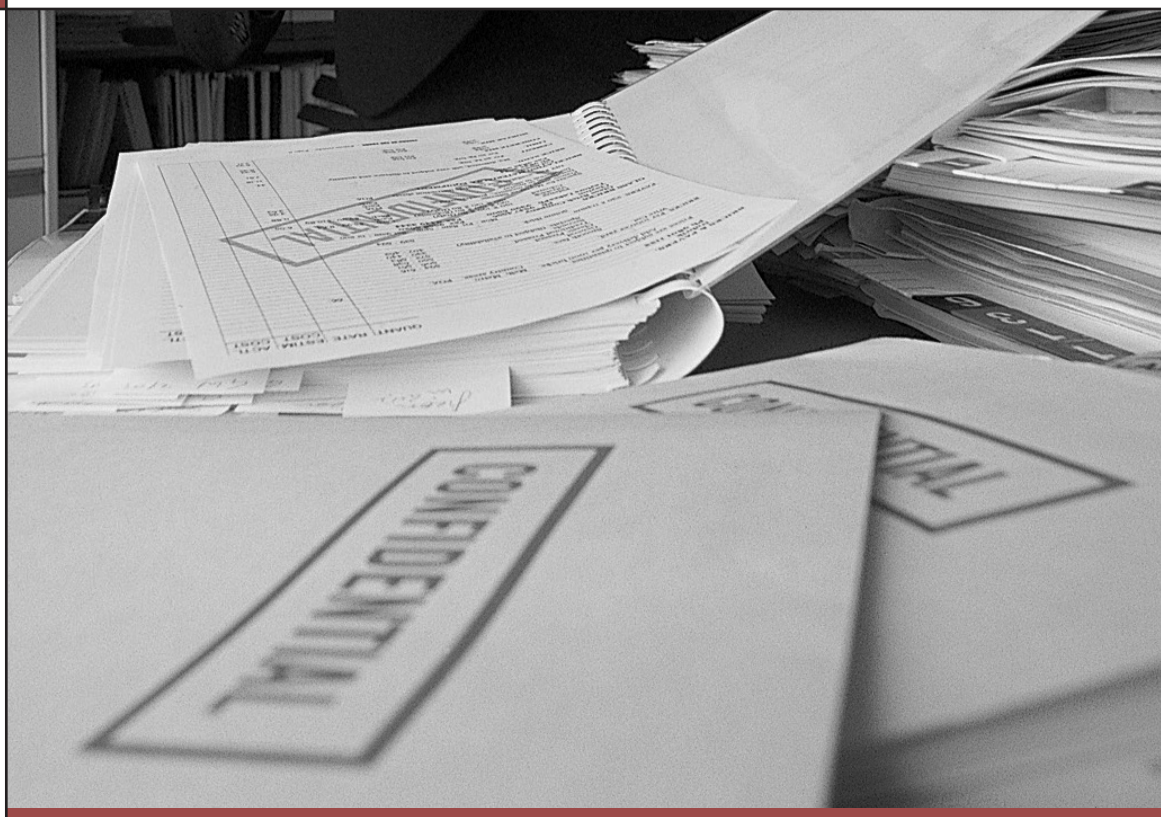
OCTOBER 2005

Transforming the Intelligence Community: Improving the Collection and Management of Information



Elaine C. Kamarck
John F. Kennedy School of Government
Harvard University

IBM Center for
The Business of Government

Transformation of Organizations Series

TRANSFORMATION OF ORGANIZATIONS SERIES

Transforming the Intelligence Community: Improving the Collection and Management of Information

Elaine C. Kamarck
John F. Kennedy School of Government
Harvard University

October 2005

IBM Center for
The Business of Government

TABLE OF CONTENTS

FOREWORD

October 2005

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, "Transforming the Intelligence Community: Improving the Collection and Management of Information," by Elaine C. Kamarck.

While Congress and the executive branch have taken a top-down view to reforming the work of the intelligence community to improve national security, Dr. Kamarck takes a bottom-up view. She stresses the importance of cultivating a new culture among frontline analysts that is based on the principles of the field of knowledge management. This field stresses the importance of combining both the implicit knowledge of individual analysts—which some call "experience and wisdom"—with the explicit knowledge developed within their organizations, such as maps and decoded messages.

To do this, Dr. Kamarck describes how the principles of knowledge management can be applied within the intelligence community. For example, she suggests approaches for creating greater access to real-time information by analysts and users, along with the strategic rotation of employees and the use of matrix management approaches. These approaches would include greater use of open, unclassified sources of information as well as adopting lessons from the Defense Department's Goldwater-Nichols reforms of the mid-1980s that led to greater integration of the military services.

While the principles in this report can be applied in many agencies, federal executives in agencies with employees on the front lines in the nation's war on terrorism will find the insights and lessons in this report well worth their time to read as they prepare their strategic approaches to more effectively manage for bottom-line results in coming years.

Albert Morales
Managing Partner
IBM Center for The Business of Government
albert.morales@us.ibm.com

Stephen Conver
Partner
IBM Business Consulting Services
sconver@us.ibm.com

EXECUTIVE SUMMARY

In the years since the end of the Cold War, the intelligence community (IC) has engaged in much soul searching but with little action. That is beginning to change in the wake of intelligence failures surrounding September 11, 2001, and in Iraq. But the solutions enacted so far, especially the creation of the Office of the Director of National Intelligence, do not get to some of the real problems in the community. The community was built to follow the Soviet monolith, and it needs fundamental reforms in the ways ordinary intelligence officers work to meet the new threats of the 21st century.

The field of knowledge management is a convenient starting point for attempting to understand what has to happen for the IC to become capable of dealing with 21st century threats. Knowledge management suggests that the IC of the future should seek to combine the tacit knowledge of the organization with its explicit knowledge. It should allow freer access to information and create ways of learning from both internal and external networks. Redundancy should be regarded as an important aspect of organizational design along with the strategic rotation of employees and matrix management. Finally, the IC should create mechanisms to learn from its mistakes and mechanisms that allow it to operate in real time in order to become capable of continuous innovation and adaptation.

The report concludes with eight recommendations aimed at building a different, more comprehensive intelligence community capable of providing its customers with knowledge about the threats that this country and the world will face in the years ahead.

Background

When the Cold War ended, the leaders of the intelligence community (IC) adjusted their assessments of national security threats to the United States to reflect the decreased threat from the Soviet Union and the increased threat from terrorism. In recognition of this new era, the intelligence community had, by the mid-1990s, created a new section to deal with the nation states that emerged in the collapse of the Soviet Union, downsized its Soviet efforts, created sections to deal with "trans-national" threats, increased its terrorism budget, and identified the threat posed by Al Qaeda.[1] The intelligence community's internal efforts were reinforced by other reform efforts in and out of government. All together in the decade after the fall of the Soviet Union and before 9/11, no fewer than 12 high-level groups had examined the IC and made recommendations for reform. Inside the government, attention to the need for change was buttressed by the Federal Bureau of Investigation's (FBI) strategic plan, *Keeping Tomorrow Safe,* and by a massive strategic planning exercise in the Central Intelligence Agency (CIA) that looked at China, the information revolution, and other aspects of the post–Cold War world.

In addition, these reports were augmented by two reports from Vice President Al Gore's National Performance Review. Outside the government, calls for change came from nine other high-level organizations. Typical of the reforms called for were these taken from the 1993 National Performance Review: "the 13 components of the intelligence community [should] act more effectively and more efficiently as a team…. [the intelligence community should] develop integrated personnel and training systems … [the intelligence community should] reassess information collection to meet new analytical challenges."[2]

Political scientist Amy Zegart reviewed all the recommendations that emerged in this decade and found that they shared common themes: "… the intelligence community's lack of coherence or 'corporateness'; insufficient human intelligence, personnel systems that failed to align intelligence needs with personnel skills or encourage information sharing; and weaknesses in setting intelligence priorities."[3] Together, Zegart counted 340 recommendations to improve U.S. intelligence capability.[4]

But of these, only 35 reforms were implemented. Clearly, throughout the 1990s, reform in the intelligence community received more lip service than action. September 11 should have changed that—but even then it took a while. In the first two years after the greatest American intelligence failure since Pearl Harbor, no one was fired and very little was changed.[5] In an historic interlude eerily reminiscent of the period between 1944 and 1947 when the FBI fought bureaucratic battles in opposition to the formation of the CIA, the period between September 11, 2001, and December 2004 saw intense bureaucratic skirmishes designed to prevent change in the intelligence community.[6] But after three years of relative inaction, a combination of factors—the failure to find weapons of mass destruction in Iraq, criticisms raised during the presidential election campaign, and intense pro-reform lobbying by victims of 9/11—finally resulted in passage of the Intelligence Reform and Terrorism Prevention Act of 2004.

Nonetheless, when change finally did happen it struck many as orthogonal to the real problems of the community. The most widely touted reform was the creation of the position of Director of National Intelligence (DNI), an idea that had been around for years and was supposed to cure the problems

What Is the Office of the Director of National Intelligence?

In late 2004, Congress passed the most comprehensive reform of the U.S. intelligence community since its formation over 50 years ago—the Intelligence Reform and Terrorism Prevention Act of 2004. A key element of this legislation was the creation of the Office of the Director of National Intelligence (ODNI) to manage across the 15 different agencies that constitute the intelligence community.

In March 2005, President George W. Bush selected former ambassador John Negroponte to serve as the first Director of National Intelligence (DNI). Director Negroponte inherited an existing staff that had previously supported the director of the Central Intelligence Agency (CIA) in his role as director of central intelligence. The CIA director, in that role, had limited authority to coordinate across the intelligence community. The new Office of the Director of National Intelligence ultimately will be expanded to as many as 300 to 500 staff members, largely drawing on existing staff from across the community. This approach was inspired by the successful Goldwater-Nichols legislation adopted in the mid-1980s to reform the Defense Department by encouraging more joint operations across the military services.

The legislation, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), also transfers to the DNI two key authorities previously held by the CIA director: providing national intelligence to policy makers (as opposed to tactical intelligence for military commanders) and heading the intelligence community, with authority to set priorities and draft a budget for national intelligence programs.

The legislation strengthens the intelligence budget authority previously held by the CIA director. It specifically stipulates that the DNI will "develop and determine" the community's budget, allows the DNI to withhold funds until recipients comply with DNI spending priorities, and, with some limits, allows the DNI to reallocate funding among programs and agencies. The DNI also is granted the authority to approve appointments to key leadership positions in the 15 agencies.

While the legislation is intended to create a stronger central intelligence authority, some observers suggest that many of its provisions could be interpreted differently. The law gives the president the authority to issue guidelines to ensure a consistent interpretation. How these guidelines evolve will ultimately determine the effectiveness of the new role of the DNI.

arising from the lack of integration among the various aspects of the intelligence community.[7] The legislation also authorized the establishment of an office—the Office of the Director of National Intelligence (ODNI)—to support this position. To date, the office is attracting experienced and talented people and its power has been reinforced by actions of the George W. Bush administration. For example, they have moved the President's Daily Brief (PDB) out of CIA and into the ODNI and extended the power of the ODNI over the FBI's intelligence budget.

But the creation of the DNI is unlikely to solve the deep operational problems the U.S. government has had anticipating the new security threats of the 21st century. In the end, passage of legislation creating the DNI was the quintessential political fix to a political problem. These kinds of fixes tend to have certain things in common: They tend to be high profile and low power. The creation of the position is trotted out as a solution to a myriad of problems that the person in that position can't possibly hope to solve, and an additional layer of bureaucracy is created between producers and consumers. And, finally, to get the legislation passed, the power in the position usually comes down to two things: (1) the power of the person in that position to persuade other powerful actors in the system to go along with him or her, and (2) the extent of presidential backing. Actual budgetary power usually turns out to be more of an illusion than a lever. This has been the experience of the "drug czar," an office created in 1988 to oversee the 50-odd federal agencies involved in the war on drugs.[8]

Thus, to date, the major organizational innovation in a community everyone agrees is in need of innovation is the creation of an office that essentially "oversees" and "coordinates" other established entities. This proposal had become the centerpiece of lobbying by members of the 9/11 Commission

Abbreviations and Acronyms

CIA	Central Intelligence Agency
DI	Directorate of Intelligence, CIA
DNI	Director of National Intelligence
DO	Directorate of Operations, CIA
FBI	Federal Bureau of Investigation
HUMINT	human intelligence
IC	intelligence community
NIC	National Intelligence Council
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
PDB	President's Daily Brief
WMD	weapons of mass destruction

who, aided by the emotional power of the families of the 9/11 victims, sought to make sure that their report was not ignored. This was ironic given that one of the major strengths of the 9/11 Commission report was the exceedingly detailed and authentic accounts of the internal workings of various government agencies—from the operational foul-ups between the CIA and FBI that resulted in Khalid al-Mihdhar and Nawaf al-Hazmi being allowed to enter the United States to the pre-9/11 interpretation of Foreign Intelligence Surveillance Act information that resulted in keeping relevant National Security Agency (NSA) and CIA information from domestic criminal investigators. In the many government foul-ups chronicled by the 9/11 Commission, few occurred as a result of insufficient budgetary authority, and many occurred as a result of bureaucratic procedures so far down in the bureaucracy that they are unlikely to be uncovered, let alone changed, by the creation of a terrorism czar. Thus, to this author and others, the organizational recommendations of the 9/11 Commission bear little or no relationship to the governmental problems that are so stunningly recounted in the text.[9]

The ODNI is likely to wield some power in the short term because so much of the Bush administration's reform agenda in the intelligence arena is associated with this innovation. But it may lack the statutory clout needed to outlast the politics of its creation. Creation of the ODNI reflects the sort of thinking best summed up by a first-century Roman satirist: "We tend to meet any new situation in life by reorganizing. And what a wonderful method it can be for creating the illusion of progress while producing confusion, inefficiency, and demoralization."[10]

What Can the Intelligence Community (IC) Learn from Knowledge Management?

So if the creation of the ODNI is unlikely by itself to achieve fundamental reform in the intelligence community, what is? The problem with the ODNI is that it deals with the very top of the community, and yet the kinds of transformations called for in the 21st century deal with how the frontline work of that community is done. In an article written for RAND, Deborah Barger argues that what is needed is a revolution in intelligence affairs similar to what took place in the military. The end objective of this revolution should lead to "changes in people's behavior and day-to-day activities."[11] This report attempts to lay out ways in which the emerging field of knowledge management can foster creative thinking about reforms at the front lines of the intelligence community, the kinds of reforms likely to change day-to-day activities. It will argue that what the 21st century policy maker will need is global knowledge that informs policy. The scope and depth of that knowledge is fundamentally different from what was needed by policy makers during the Cold War and will thus require a frontline transformation of existing intelligence organizations and the creation of new ones. The creation of the ODNI will not guarantee that these reforms happen. However, if the experienced officials who are now beginning to staff the ODNI hope to escape becoming the 21st century version of the drug czar, they would be well advised to make fundamental organizational transformation their primary goal.

So how can the new and emergent field of knowledge management help in fundamentally restructuring the front lines of the intelligence organizations? Knowledge management studies have examined how private sector companies create and use knowledge as part and parcel of their organizational culture. It is a common sense methodology that attempts to organize the valuable internal information of a company, much of which is experiential, and integrate it into the more formal information flows in ways that help the company stay competitive. Corporate giants like Motorola, Microsoft, IBM, and General Electric have worked hard at the integration of internal knowledge. By organizing in ways that are designed to maximize the creation of new knowledge, these companies hope to apply the knowledge of the company to innovations in both products and processes.

Knowledge management arises in response to two characteristics that the competitive global information economy shares with the national security community: uncertainty and data overload. Much of the work on knowledge management in the corporate community began in the late 1980s and early 1990s when it emerged as a consequence of both globalization and the information revolution.[12] Knowledge management is an integral part of an economy where "the only certainty is uncertainty, the one sure source of lasting competitive advantage is knowledge."[13] In addition, knowledge management tries to cope with the paradox of data overload. In the 21st century, computers allow us to collect and manage huge amounts of data, but unless the data lead to changes in organizational structure and changes in work, they won't do anyone much good. The management guru Peter Drucker writes, "as soon as a company takes the first tentative steps from data to information, its decision processes, management structure, and even the way its work gets done begin to be transformed."[14]

The IC of the 21st century will also have to cope with uncertainty and data overload. Gone is the stability of the nation-state era when intelligence

could be defined as ascertaining the capacities and the intentions of other nation states—and the work of intelligence could be operationalized into more or less discrete tasks such as stealing state secrets or counting armored tanks. Divining the capacities and intentions of other national actors was never easy, but at least it was bounded. This work is not going away. In fact, with the rise of China as a potential adversary, it may be more important than ever. But in an era when loose networks of terrorists, working in autonomous cells, can bring global cities to their knees and threaten populations with nuclear or biological weapons, the very source of the national security threat is uncertain, and the IC has to develop an additional paradigm to deal with non-state threats. Terrorism is not the only non-state threat. We have national security concerns about proliferation, organized-crime trafficking in strategic materials, chronic conflicts, genocidal outbursts that demand intervention, failing states, and destabilization from disease outbreaks, to name but a few.

Uncertainty means that we need to conceptualize the IC as a community that provides knowledge and makes sense of the world to policy makers—a function fundamentally different from conceptualizing the IC as a community that provides information. The IC of the 20th century could provide information because it was built around an enemy that was known, stable, and bounded. Because the Soviet empire was, by and large, a closed system, intelligence was developed and then defined around the stealing of secrets. Stealing secrets on behalf of the state was the classic work of espionage. In the Cold War, the IC knew who the enemy was and what had to be learned about them.

There were enormous advantages to this stability. For example, the IC knew what languages spies and analysts would need—Russian, Russian, and more Russian. There was widespread consensus on the name, location, and threat posed by the enemy, and this consensus allowed Congress to give the IC the benefit of the doubt when it came to operational issues. Once that consensus on the enemy was gone, Congress would become irate over previously tolerated practices such as the recruitment of unsavory characters in Central America. The unintended consequence was to generate a chilling effect on the CIA and to create what more than one insider has referred to as a risk-averse culture in the very business—spying—where risk is needed. And, finally, because the Soviet Union was a closed system, the IC did not have to compete with CNN, websites, or bloggers; it had a near virtual monopoly on information about Soviet intentions and capabilities.

According to one former intelligence community officer, "To a certain extent, the Soviet Union is still alive and well in the cultures and in the bureaucratic authorities of the IC."[15] In contrast to the Soviet threat, many of the national security threats of the 21st century are not stable, they are not bounded, and, in fact, they are not even known. A small example of this is the fact that President Bush no longer talks about Osama bin Laden. While his detractors maintain that this is because bin Laden is still at large, there is a more fundamental reason. In the years since the 9/11 attacks, we have come to understand that terrorist threats do not at all resemble the highly organized Soviet threat of the 20th century. Officials from the intelligence services of many different countries agree on the fact that killing bin Laden, capturing his associates, or bombing his camps will not end the threat. CIA Director Porter Goss recently told NBC News: "Certainly the Al Qaeda organization represents the embodiment of some kind of a network of global terrorism…. But we think in a kind of organized Western mind about what a network would look like. It's not. It's very amorphous. Some of it is self-starting. There are cells here and there are cells there that are loosely related."[16] In the Western mind, "we reduce conflict to leaders and tend to believe that if we get rid of the leaders, we get rid of the problem."[17] This is not so with many 21st century threats.[18]

Second, the unparalleled amount of data collected by the U.S. government doesn't necessarily make us smarter or safer. Sad testament to this phenomenon was the fact that within days of the attacks of September 11, every newspaper in America had photographs and biographical information on all the hijackers. The amazing speed with which this information was pulled together was one simple reminder that while we had the data on the hijackers, the systems in place would not allow it to be translated into the kind of knowledge that could have allowed us to predict threats and prevent catastrophe.

Every day the U.S. government collects vast amounts of information via its satellites. And yet there are backlogs of conversations waiting to be translated

and backlogs of satellite photographs to be looked at.[19] For instance, one expert described the data-overload problem as follows: "In FY '03, with the Global War on Terrorism and all the data that come out of Afghanistan, plus all of the criminal and fraud data we processed in the lab, if we printed it and stacked it, it would have been over 18,000 Washington Monuments.… We are packing more and more data in smaller and smaller places, charging less and less for it, and we are putting them in more and more devices, and we can't keep up."[20]

These changes in the post–Cold War national security picture have resulted in the conviction within much of the intelligence community that "our fundamental business objective will change from intelligence, that is the stealing of secrets, to that of providing information, information that is from both open and closed sources, that can be used by policy makers and the public at large."[21] This is, frankly, a very different and much more complex business than stealing secrets from the Soviets, and it involves reforms at the front lines of the community. And while the author is the first to admit that there are profound differences between private and public sector organizations, the wisdom gleaned from the private sector should be used to stimulate thinking about public sector reforms in the critically important area of intelligence for national security.

Eight themes appear and re-appear in the knowledge management literature that suggest lines of reform in the intelligence community. They are as follows:

1. Creating new knowledge requires tapping the tacit knowledge of an organization and combining it with the organization's explicit knowledge.
2. Knowledge-producing organizations allow free access to information.
3. In knowledge-producing organizations, there is extensive learning from others and employees are embedded in outside networks.
4. In knowledge-producing organizations, redundancy is not regarded as waste, rather it is regarded as a key aspect of organizational design.
5. Knowledge-producing organizations engage in "strategic rotation" of their employees.
6. In knowledge-producing organizations, sequence is replaced by synchrony.
7. In knowledge-producing organizations, systems exist that allow for learning from past experience.
8. Knowledge-producing organizations engage in continuous innovation.

Tacit and Explicit Knowledge

The intelligence community needs to develop ways to combine tacit and explicit knowledge.

Tacit knowledge is highly personal, hard to formalize, and difficult to communicate to others, in contrast to explicit knowledge, which is formalized, rational, and easily communicated to others. Real knowledge usually involves the meaningful interaction of the two. There is a significant amount of literature on tacit knowledge, sometimes called "implicit" knowledge. Tacit knowledge is defined as "a natural concept that refers to a type of knowledge that has been shown in previous research to be useful in predicting performance in real-world endeavors." It is a "key to intelligent behavior in practical settings, it is the practical know-how that one needs in order to succeed."[22] Implicit learning is defined as: "the non-intentional, automatic acquisition of knowledge about structural relations between objects or events."[23]

Tacit knowledge has been shown to be critical to a wide variety of fields, from law to medicine, from management to teaching, and from sales to the military.[24] In their study of military leadership, Horvath et al. conclude that this knowledge "operationalized or supplemented the doctrinal guidelines.… [And was] learned over time through experience in real-world settings."[25] And in a recent best-seller titled *Blink: The Power of Thinking Without Thinking,* Malcolm Gladwell popularizes much of this research by weaving together stories of how the unconscious knowledge of experts is exercised nearly instantaneously.[26]

But as important and fundamental as tacit knowledge is to highly skilled work, organizations have a hard time capturing and using it. An exception is the Matsushita Electronics Company. Ikujiro Nonaka, a leading expert on knowledge management in the

private sector, tells how Matsushita set out to design a home bread-making machine. They were having trouble getting the machine to knead the dough correctly, so the company sent an employee to the bakery known to make the best bread in Tokyo to study with the chief baker. The best baker in Tokyo had a certain technique, developed over many years, for kneading bread. This technique, pure tactic knowledge on the part of the master baker, needed to be transferred to the machine's kneading arm. After studying his methods and observing the baker, she was able to go back to the company and work with the engineers to design a machine that more closely reproduced the baker's style. The result was the best-selling machine on the market.[27]

On one level, organizations value tacit knowledge. It is one of the reasons why CEOs so often come up through the "line" portions of the corporations and why in retailing even the highest-level executives are expected to "walk the floor" and have some experience in sales. Much of modern management science preaches flattening organizations, listening to the "edge" of the organizations, empowering the front lines, and other strategies that are attempts to capture the tacit knowledge usually held by those closest to the customers. But creating organizations that routinely and effectively integrate tacit knowledge with explicit knowledge and use it for continuous improvement is not so easy. Writing in the *California Management Review,* Liam Fahey and Laurence Prusak conclude, "in spite of the emphasis upon tacit knowledge in both traditional epistemology and the recent knowledge management literature, organizations seem especially reluctant to grapple with its management."[28]

This is very much the case in the intelligence community. In the IC, the possessors of tacit knowledge are the people who work in country in the CIA's Directorate of Operations, otherwise known as the "handlers" of spies and the spies themselves. Because the collectors of intelligence in the field live in a foreign country, speak the native language, and interact with the locals, they tend to possess the tacit knowledge that, in combination with explicit knowledge, is so critical to figuring out what is going on. That is one of the reasons why almost all intelligence reform commissions have called for more spies, or human intelligence (HUMINT.) And that is why one of the most disastrous assumptions of the post–Cold War era was that the U.S. could do with fewer human sources of intelligence and more satellites.

Since 9/11, recruiting in the Directorate of Operations has been robust, and lip service, at least, has been given to the need to build up HUMINT.[29] But the literature of knowledge management suggests that more spies won't necessarily produce better intelligence if the tacit knowledge they acquire along the way isn't sufficiently integrated with the explicit knowledge that the analysts back in Langley collect. This is a challenge in any organization, but it is an even bigger challenge in an organization that has built a wall between operations and analysis and considered that wall a virtue. In a recently declassified essay from 1961, a member of the IC who was critical of the separation of spies from analysts describes the separation of operations and analysis as based on two assumptions. First, the analyst is presumed to be better at the job of evaluation—even though the collector makes decisions every day on what to pursue and what to ignore that are part and parcel of the evaluation process. Secondly, the collector is assumed to be undependable "as a maker of objective judgments" because of his contact with his sources and his personal interest in the success of his operations.[30] A more recent member of the intelligence community adds that while no one wanted analysts running cases, the distance the analytical community maintained from reporting sources grew larger and larger on the grounds that that was the only way to preserve objectivity.

The lack of trust between the Directorate of Intelligence (DI) and the Directorate of Operations (DO) at the CIA was fully reciprocal. Just as analysts didn't trust the judgment of collectors, collectors didn't trust analysts. And even if they did, very few members of the DO wanted to add more people to the inner circle of knowledge and operations.

While there are, no doubt, merits to these arguments, they have been used to justify a division between the DO and the DI that has grown so large as to be counterproductive, especially in a world where the enemy is not constant and thus the prediction of surprise is difficult. A CIA operative in Tehran in the late 1970s recalls arguing for permission to use the word *revolution* in a communiqué to Washington in February of 1978. Later that year, the chief analyst for Iran wrote the following, now famous (or infamous) report, stating that Iran is "not

in a revolutionary or even pre-revolutionary stage."[31] His experience recalls the admonition of the operative who, writing in 1961, explained, "Many of the indicators simply do not speak to the analyst in his remote office with the same ring they have for the collector experiencing them in the field."[32] What is lost is the tacit knowledge of the collector.

The extent to which this knowledge is lost is even more critical in a world where security threats are constantly changing and unbounded. One former security expert posed the question as follows: "The nation state tended to specialize and professionalize such things. It drew a bright line between collectors and analysts. The market state won't put up with that. It will not allow experts to have the final say. It wants more…."[33]

The need for more knowledge means that the intelligence community will also have to expand its definition of the community to include more collectors of information than those typically found in the DO. The holders of relevant tacit knowledge are not just spies but police officers on the beat in every city and town in the world. Volumes have been written about the conflicts between "cops and spies." But usually these refer to the decades-long conflicts over turf between the FBI and CIA. The fact is that in the 21st century we will need to depend not just on FBI agents but on ordinary cops on the beat in cities around the world.

Experienced police know when something is wrong. A Philippine policewoman named Aida Farsical trusted her intuition one night in 1995 when a routine fire alarm went off in Manila. Her "intuition" led to the arrest and interruption of the famous "Bojinka" plot, which, had it been successful, would have resulted in fatal explosions aboard 11 long-haul airline flights between the United States and Asia.[34] The homegrown American terrorist Timothy McVeigh, who was executed for blowing up the Murrah Federal Building in Oklahoma City, was caught by Charlie Hanger, an alert Oklahoma highway patrolman.[35] And the "Millennium Plot" to blow up Los Angeles Airport was disrupted by Diana Dean, an alert customs agent at the Port Angeles border crossing from Canada into the United States.[36] In the past three years, British police have broken up at least two cells, and maybe as many as five cells, that were planning major attacks—even though, sadly, they failed to interrupt the July 2005 attack.[37] And the New York City Police Department, with officers based around the world and specialized anti-terror teams that integrate what's going on in Pakistan as well as what's going on in the Bronx, is a model for the new role of big-city police departments in the IC.[38]

The "street smarts" of cops on the beat may constitute the ultimate in tacit knowledge and the best chance to avert catastrophes. Capturing that knowledge is the first of many challenges confronting the front lines of the intelligence community.

Implications for Intelligence Community Actions

The CIA especially, but the larger IC as well, needs to focus on its core mission—the creation of valuable secret knowledge that makes sense out of the various perplexing and unknown threats of the 21st century. This will involve not just more spies but the creation of a closer relationship between collectors and analysts, one that will allow the organization to capture both tacit and explicit knowledge. Some have suggested having analysts spend more of their working life in country than they currently do and, simultaneously, breaking down the walls that exist between collectors and analysts so that they have more of a collaborative relationship.

An organization more tightly focused on secrets still needs analysts who are dealing with open source data as well as secret information. One experienced intelligence professional summarized the symbiotic relationship by using the metaphor of a jigsaw puzzle: "you have this nifty piece of the jigsaw puzzle, a very important piece, a secret. But you don't know where the hell it fits. But the open source people may give you the picture on the cover of the box, and now, 'aha, I see the whole picture, that's where it fits.' And yet the open source people, trying to look at this picture, may have drawn it without this key piece of the puzzle; they may have to actually rearrange the picture if they find it."[39] Thus, focusing the CIA on the collection of valuable secrets involves the kind of open source knowledge that many analysts currently use, but it should be integrated with secret knowledge in a way that makes the secrets more valuable.

Access to Information

The intelligence community needs to free up access to information.

All the techniques of knowledge management depend upon open access to information within the company. In companies that work to create knowledge, there are no differentials in information between those at the top, those in the middle, and those on the front lines. Nonaka argues, "When information differentials exist, members of an organization can no longer interact on equal terms, which hinders the search for different interpretations of new knowledge."[40] The literature on knowledge management advocates establishing knowledge networks, knowledge repositories, and communities of practice. In recent years, principles of just-in-time management have been employed in knowledge-heavy industries such as healthcare to reduce the amount of time knowledge workers have to spend to stay current.[41]

One of the most common organizational mistakes is to treat knowledge as if it existed "predominantly outside the heads of individuals." This problem, identified by Fahey and Prusak, stems from the difficulties organizations have understanding that "data" is no substitute for knowledge. Information technology allows organizations to build elaborate knowledge bases and search engines, and in the course of this data management, they tend to forget that knowledge does not have a life of its own—it only exists when people use it![42]

If ordinary private sector organizations have trouble sharing knowledge in ways needed to turn data into knowledge, imagine how much more complex this problem becomes when much of the data is secret. Secrecy impedes the free flow of information. The famous "need to know" dictum only works in a world where you know what you need to know. In a world characterized by a high degree of flux and uncertainty, it is hard to know what a given analyst or consumer needs to know. Bruce D. Berkowitz and Allan E. Goodman, two of the most thoughtful intelligence experts around, write, "A culture that assumes facts are secret until determined otherwise can have all sorts of pernicious effects…. Secrecy runs counter to the essence of the information revolution, where the free flow of information drives productivity and creativity.… Organizations in the Information Age take advantage of such ideas by operating as open, fluid networks."[43] Echoing these sentiments, Congresswoman Jane Harman, ranking Democrat on the House Special Intelligence Committee, suggests moving from a "need to know" culture to a "need to share" culture.

In addition, it is possible that, in the Information Age, the sheer number of covert items needed to put together a security puzzle may have decreased relative to the number of overt items readily available. During the Cold War, the Soviet Union worked hard to keep both its intentions and its capabilities secret. In the war against Osama bin Laden, the capabilities are hidden but the intentions are not. In *Imperial Hubris*, a U.S. intelligence official, critical of the lack of understanding that the U.S. government has shown in its policies in the Muslim world, spends a large part of his book showing how the bulk of Osama bin Laden's intentions were public and available for all to see—as was information on Afghanistan. "The great bulk of it [information on the mujadeen] requires no access to signals intelligence, clandestine collection, diplomatic reporting, or satellite imagery. A trip to the local library probably would suffice.…"[44]

One journalist who covers intelligence describes the changing relative value of secrets as follows: "We live in what I sometimes call the age of overt action. Most of the things that matter in the world today happen in open space, in front of the television cameras."[45] Yet, in spite of these changes, the intelligence community clings to secrecy. Even internal processes designed to balance the risk of revealing secrets against the need to share information tend to err on the side of protecting secrets. One student of the process summed up the problem as follows: "Let's face it, our business is collecting and protecting secrets, but the secrets that we collect are not useful unless we share them appropriately. As our secrets become more and more time critical, it is imperative that we provide this information to others quickly and seamlessly, but we must still protect our secrets."[46]

Secrecy prevents the IC from turning data into knowledge, and it reinforces the organizational stovepipes that plague all large organizations—public and private. This is dangerous in two respects. First of all, secrecy tends to hide, or at least obscure, the analysts' visibility into the reli-

ability of sources. An internal intelligence community report, commenting on what went wrong with intelligence in Iraq, concluded that all too often clandestine reporting used different descriptions for the same source—with the result that analysts were led to believe they had corroborative information from more sources than was actually the case.[47] In addition, excessive secrecy allows analysts to rely on unreliable sources. One of the most famous is called "Curveball," an Iraqi defector who provided information on supposed biological weapons in Iraq to the Defense Department's intelligence office and whose claims were not discredited until 15 months after they were featured prominently in Secretary of State Colin Powell's address to the United Nations that made the case for war.[48] Secrecy within the government and the paucity, indeed absence, of other real information—contextual or otherwise—on Saddam Hussein's government allowed the government to draw conclusions that were to prove false.

The second problem with secrecy within the intelligence community is that it tends to reinforce organizational stovepipes. Within the community there are groups that focus on regions and countries, and groups organized around functional expertise and crisis response. Two different studies of why the IC failed in its assessment of weapons of mass destruction (WMD) in Iraq cite the failure to meld expertise on WMD with expertise on the political and cultural situation in Iraq. An internal intelligence community report concluded that in the intelligence world, technical analysis came to dominate regional analysis—resulting in a lack of perspective and comprehensive understanding of the Iraqi target.[49] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (hereinafter referred to as the Silberman/Robb report for its chairs, Laurence Silberman and Chuck Robb) concludes, "In short, the intelligence community did not sufficiently understand the political dynamics of Saddam Hussein's Iraq, and as a consequence did not understand the political and economic pressures that led to his decision to destroy his WMD stockpiles while continuing to obfuscate about Iraq's possession of WMD."[50]

Transnational threats cannot be fully understood without also understanding the geography in which they thrive—be they the Muslim ghettos of British industrial cities or the failed states of Africa. But understanding the "mysteries" as opposed to the "puzzles" of the 21st century requires the constant integration of different kinds of information since, as Gregory F. Treverton writes, "most of the critical questions facing American foreign policy are mysteries."[51] Studies of high-reliability organizations find that they regularly bring different departments together in order to better understand problems. Secrecy is inimical to the kind of cross-organizational cooperation found in organizations that create knowledge.

Finally, secrecy allows the IC to hide its mistakes and avoid change. This is one of the major differences between bureaucracies in the IC and bureaucracies on the domestic side of the government. Domestic agencies have a very hard time hiding their mistakes. The IC doesn't.

Implications for Intelligence Community Action

As we have seen, secrecy is a major impediment to knowledge sharing. As a first step, the IC as a whole should try to standardize its security clearances and its classification processes within the federal government. This will allow for the creation of internal "communities of practice," or "directories" of people who have substantive knowledge about specific issues. Most practitioners of organizational transformation begin with what is commonly referred to as "the low-hanging fruit"—meaning those things that are relatively straightforward and that signal the direction in which the organization should move. Removing obstacles to communication within the 15 federal IC entities is low-hanging fruit. It is straightforward and would signal a new era of "jointness" in the IC.

Years ago, a reform commission called the Murphy Commission on Governmental Reorganization called for a "unified personnel system for the foreign service agencies, designed to eliminate rivalries and provide a mechanism to support all non-military overseas options. In effect, the channels through which the State Department, the Central Intelligence Agency, the International Communications Agency, [Unites States Information Agency], and the Agency for International Development now recruit, train, and deploy their junior officers would be replaced

by a single body."[52] While it may not be necessary to establish a unified personnel system, it is clearly time for more uniformity in the clearance system, and all new IT systems should be compatible across agencies.

External Networks

The intelligence community should make use of external networks.

The global trend in manufacturing has been to produce fewer and fewer parts of a product in house, instead relying on a network of subcontractors. For instance, corporate giants like Ford Motor Company, General Motors, and Dell find themselves embedded in "value networks" or "production networks." Timothy Sturgeon of the Massachusetts Institute of Technology writes that "a network highlights the nature and extent of the inter-firm relationships that bind sets of firms into larger economic groups."[53] The trend toward networks can be seen in the public sector as well, where government has contracted out much of its social service work to nonprofit organizations, for-profit organizations, and even churches.[54]

The organizational move to networks in the private sector and in the public sector reflects the desire for both specialization and innovation that allow for the flexibility so central to organizations in the Information Age. Rather than designing automobile interiors themselves, Ford Motor Company finds it makes sense to contract out interiors to companies that specialize in interiors. Rather than trying to figure out a regime for getting welfare mothers back to work, state governments routinely contract out that work to a variety of providers who focus on those programs.

The "production network" in the creation of relevant national security information in the 21st century will need to involve many actors outside the IC itself. But if differences in security clearances and rules hamper the sharing of information *within* the United States federal government, those rules and the culture they reinforce are fatal to the sharing of information *outside* the IC. Creating collaborative networks within and among government intelligence and law enforcement is difficult enough. As the IC is called upon to provide a higher level of cultural expertise and analysis, it will be called upon to monitor the cyber café *and* the defense minister's office. The IC already relies on large amounts of open source data, and its reliance on open sources is likely to increase, not decrease. The IC will be called upon to distinguish fact from fiction in this increasingly open and diverse world. If, as discussed earlier, it is important to understand the reliability of clandestine sources such as the infamous "Curveball," it is equally important to be able to sort out fact from disinformation from outright fiction on the Internet.

This involves a great deal of work—much of it new. The organizational solution is to create the equivalent of a production network for the production of intelligence that can take advantage of expertise and perspectives that may not reside within intelligence or law enforcement structures. To do this effectively, the IC will have to rely on open source material and embed itself in the networks of journalists, academics, businesspeople, political consultants, and scientists that already have the experience needed to sort out complexity in the world.

However, in the course of trying to create these networks, the IC will come up against people who do not have—and may not want—security clearances. While certain portions of the intelligence community develop relationships with professionals who have relevant (usually country-based) expertise, there is a limit on the number of people who wish to have regular contact with a secret agency. For journalists, identification with the IC could cause sources to dry up—quickly. For academics, it could hamper the perception of their objectivity. For American business, it could cut sales. And for the American political consultants who increasingly advise political leaders in countries around the world, and who could offer incredibly important insights into the intentions of national leaders, it could be the end of their business.[55] And since, as the nuclear non-proliferation expert Ash Carter points out, the government has had and will continue to have a hard time recruiting and retaining top scientific talent, given the more lucrative prospects in private industry, it will need to "forge better links with the outside scientific community so that advice and insight are 'on call.' "[56] This conclusion is true not just for nuclear experts but for experts in the spread of diseases that, intentionally or unintentionally, could constitute a new and extraordinarily

Excerpts from "Building a Comprehensive Open Source Intelligence Capability"

By W. Scott Gould

Overview

The WMD Commission,[57] Congress, and the President have made the case for improving the open source intelligence capabilities of the intelligence community. Now the intelligence community faces the challenge of designing an open source capability that will incorporate open source intelligence into virtually all of its products. This IBM white paper proposes a model for creating a Directorate of Open Source Intelligence (DOSI) that is fully integrated into the intelligence community and will facilitate cooperation and collaboration among the constituent agencies of the intelligence community, other federal agencies, state and local governments, and the private sector.

The intelligence community (IC) is already overwhelmed with incoming information, and additional data alone will not necessarily improve the analysts' ability to provide predictive, timely intelligence to the warfighter and policy maker. The IBM white paper recommends the organizational structure, business processes, and human and technical capabilities required to build a comprehensive, efficient open source intelligence capability. Embedded in these structures, processes, and requirements is the recognition that frontline intelligence analysts need better tools to cut through the clutter. Consequently, training and a constantly running, adaptive, automatable, and customizable technology solution will be central to the utility of the capability.

Why Open Source Intelligence Is Now Needed

The information revolution of the past 20 years has resulted in a huge shift of information into the public domain. Today, the amount of open source information[58] accessible to the intelligence community is immense and rapidly expanding. It includes a wide variety of web-based materials (blogs, online publications, and commercially available databases), printed materials (pamphlets and underground newspapers), audio and video feeds (television and radio broadcasts and taped public speeches), and imagery (photographs and commercial satellite images).

This open source information is a powerful resource for the intelligence community, giving analysts a new window into the outside world. Beyond obvious functions such as monitoring extremist websites, open source information and tools can provide a new depth of understanding into the societal, cultural, and political dynamics and events taking place in countries around the world. The context or background developed through this enhanced understanding has the potential to inform and improve the full range of intelligence products.

Unfortunately, not only is much open source information going uncollected, but also analysts do not have the tools they need to successfully exploit such an overwhelming array of data. It is impractical to hope that the U.S. intelligence community would ever be able to collect and analyze all of the information that is available. However, with the correct policies and resources, the intelligence community has the opportunity to vastly increase its exploitation of open source information. Further, with the proper analytical and collaboration tools, the intelligence community's resources can be leveraged to better target the highest value open source information.

What an Open Source Model Would Look Like

Open source information is accessed or collected from a vast array of sources on a prioritized basis. Raw information is immediately made available to analysts throughout the intelligence community. Analysts are given access to customizable and automatable analytical tools including machine translation, knowledge discovery, trend analysis, and social-network analysis tools to allow them to cut through the clutter. Training on efficient and effective use of these tools will be the key.

The model calls for a small cadre of open source intelligence (OSINT) specialists who will develop specialized OSINT products, best practices, and training programs for the rest of the community. The OSINT specialists will also build and administer a network of civilian experts, both foreign and domestic, cleared and uncleared, who can provide cultural context and intelligence. This resource would be available to all members of the IC.

Finally, for the new open source capability to be successful, its management must be centralized and empowered. Strong central management is needed to overcome the traditional skepticism of the community toward OSINT and to make sure this resource is fully integrated into the intelligence process throughout the community. Centralization will provide important economies of scale when dealing with vital technology and policy issues.

W. Scott Gould is Vice President, Public Sector Strategy and Change, IBM Business Consulting Services. His e-mail: w.scott.gould@us.ibm.com.

To read the full paper, go to www.businessofgovernment.org/gli.

disruptive national security threat. Thus, to truly take advantage of networks in the creation of relevant national security knowledge, we may need to turn to new organizational forms outside of the IC.

Implications for Intelligence Community Action

Embedding the IC in external networks is difficult. The IC needs to look outward, toward collaborations with the intelligence services of other nations, and inward, toward collaborations with state and local law enforcement entities. In a recent meeting of intelligence professionals in Madrid, the participants concluded, "It is the duty of all nations to maintain their own security, but it is also their duty to actively assist in the security of all other nations—terrorism threatens everyone's security."[59] They suggest the creation of regional centers for analysis and the review of clearance and classification regimes.

In addition, the IC needs to figure out how to capture the tacit and explicit knowledge of police forces and state troopers in the United States. It has been suggested that 1 to 2 percent of the approximately 600,000 to 700,000 police officers in the country be given special training and a technology to tie them together with the federal IC as a means of capturing the street smarts of those who are most likely to come across terrorist cells.[60]

But when it comes to capturing the relevant knowledge that resides in the private sector—be it in business, academia, or journalism—it's not as simple as the creation of a network and the reform of classification. Some people will never want to be associated with a spy organization, especially one that, as appears likely, will conduct more and more clandestine operations as time goes by. And yet there is an enormous amount of open source information that has relevance for 21st century threats. The Silberman/Robb commission stated, "there is not yet an institutionalized, effective method to exploit open source resources that would have allowed a better understanding of developments in Iraq."[61] They recommend creation of a small cadre of open source analysts in the ODNI.[62]

Many other dedicated intelligence professionals share this concern about the need to increase open source collection and analysis by, for example, monitoring the bloggosphere. But at some point one has to wonder if we aren't asking the current IC—especially the CIA—to simply do too much. We want more and better HUMINT, which we can get only if we have analysis that can guide collection and put it in context. And we want more and more analysis of a huge open source world, where much of the data might be intentionally or unintentionally misleading. The answer to the latter dilemma is to create networks of experts who are outside the IC. But is it realistic to assume that an effective open source capacity can be built in a secret organization?

My conclusion is no. While secrecy may have gone too far in some instances, secrecy is here to stay. Graham Allison argues that the only way to prevent a nuclear terrorist disaster is to increase our stock of "shooters"—people who can carry out targeted, covert operations—and espionage.[63] To the extent that the capacity for covert action remains in the CIA and is enhanced, Pakistani professors, Afghan journalists, and others that the United States may wish to learn from will have trouble even getting into the building—assuming they even want to try. And those who would want to try we may not want. Al Qaeda would like to infiltrate the CIA—as many as 40 suspicious individuals have apparently tried just that in recent months.[64]

Thus, rather than attempt to load on to a secret organization the job of analyzing open source information, we should bite the bullet and create a new, open source analytic arm in the U.S. government. This could be located in a variety of places, but one logical place is in the State Department as a supporting staff in the office of the undersecretary for public diplomacy. This is a new job. Given the growing hatred toward Americans in certain parts of the world, it is a job that has yet to be done well. To do that job effectively, the undersecretary needs a lot more than a background selling soap. He or she needs the deep cultural analysis and understanding that can only come from tapping into a wide variety of non-governmental networks. This staff should be distinct from the CIA, the DNI, and the State Department's Bureau of Intelligence and Research. It should not have access to secret information. If it is seen as a front for the CIA, then it will have difficulty building the open source networks it needs.

Others have suggested that the government create a new agency that would conduct open source

analysis for the government as a whole, along the lines of the Congressional Research Service or existing federally funded research and development centers (FFRDCs) such as RAND and the Institute for Defense Analyses.[65] And yet this new open source organization should be responsible for the creation of a product that is seen regularly by the same policy makers who view the secret products being produced by CIA/ODNI. In addition to cultural analysis that bears on national security questions, a purely open source organization can incorporate the health and scientific community to help policy makers monitor potential global instability resulting from environmental or health degradation. The job of reconciling open source and secret data must ultimately fall with the president and his designees—in this instance, the National Security Council.

Redundancy

The intelligence community needs to value redundancy.

In knowledge-producing organizations, redundancy is not considered waste; it is looked upon as a key aspect of organizational design. In companies, redundancy is used to create internal competition. At Canon, for instance, "The company organizes product-development teams according to 'the principle of internal competition.' A team is divided into competing groups that develop different approaches to the same project and then argue over the advantages and disadvantages of their proposals. This encourages the team to look at a project from a variety of perspectives. Teams work on the same product and then argue over aspects of product design."[66]

In the U.S. business culture, redundancy in product development fits the cultural beliefs in the value of competition. Thus, many companies have developed strategies designed to get parts of their organizations to compete against other parts. However, the value of redundancy and internal competition depends on how it is managed. In their research, the organizational theorists Jeffrey Pfeffer and Robert Sutton found that "internal competitions didn't just harm the losers. They harmed everyone who had a stake in the organization."[67] They go on to urge caution in the use of internal competition.

In the intelligence community, as in the corporate world, redundancy can be a blessing or a curse, depending on how it is managed. The motivating factor for the creation of the ODNI was the fact that 15 agencies in the U.S. government were involved in intelligence work. Somehow the assumption was that if they were better coordinated, the intelligence would be better. This argument fits some intelligence failures but misses many others. In the case of 9/11, it could be argued that the various pieces of the puzzle might have come together if there were one center such as the new Terrorist Threat Integration Center or the new ODNI—although much of the relevant data may not have made it that far up the food chain. On the other hand, some of the criticism of the 9/11 intelligence failure and much of the criticism of the Iraq intelligence failure stem from the absence of competition in the production of intelligence estimates. "Group think" and the "continuation of basic trends" are responsible for many failures. In the case of 9/11, the assumption was that Osama bin Laden would strike outside the United States. In the case of Iraq, "collectors of intelligence absorbed the prevailing analytic consensus and tended to reject or ignore contrary information. The result was 'tunnel vision' focusing on the intelligence community's assumptions."[68]

The problem of group think is not new. "The most distinguishing characteristic of failed estimates—the Sino-Soviet split, the development of the ALFA submarine, the Qadhafi takeover in Libya, the OPEC [Organization of Petroleum Exporting Countries] price increase, the revolutionary transformation of Ethiopia, the Soviet invasion of Afghanistan, or the destruction of the shah's Iran—was that it involved historical discontinuity, and, in the early stages, apparently unlikely outcomes…. Analysts of the period clearly lacked a doctrine or a model for coping with improbable outcomes."[69] In the case of Israel's failure to predict the 1973 Yom Kippur War, group think around the conditions under which Egypt would attack were so strong that Ephraim Kahana writes, tongue in cheek, that "even if President Sadat himself met Mrs. Meir and informed her that he was about to hurl his army against Israel, Meir would probably ask him if he had long-range bombers and Scud missiles…. Hearing President Sadat reply in the negative, Mrs. Meir would no doubt say, 'Okay, when you get these weapons come and see me again and we'll talk.' "[70]

The problem before the IC is to develop processes that overcome the powerful tendencies toward

group think without asphyxiating the internal cooperation so necessary to the production of knowledge. One solution is to institutionalize competitive analysis so that it becomes a feature of every intelligence product from the President's Daily Brief to the National Intelligence Estimates. A high-level group of intelligence professionals concluded that, to the extent alternative analysis is used, it is episodic, "tacked on" to conventional analysis instead of being an essential component and not particularly effective in influencing the policy process.[71] Perhaps that is why, in spite of the fact that alternative analysis was supposed to be standard practice, Congress recently passed legislation giving the DNI the authority to enforce alternative analysis of intelligence products.[72]

Another strategy for introducing redundancy into the intelligence product is to mandate an alternative narrative, that is, another explanation for the same pieces of information. In addition, it may be time to add other competitive intelligence products to the President's Daily Brief. The tradition of presenting only one PDB to the president and other policy makers—and the resultant pressure to forge consensus—results in a loss of information for the very person who needs it most. Building effective redundancy into the IC will involve changes in its products and in the ways consumers use and understand them. There are some early signs of change in this direction. Apparently President Bush has recently begun to receive a variety of different intelligence reports and, prompted by the findings of the Silberman/Robb report, the new DNI is looking for ways "to highlight differences among analysts at various agencies."[73]

Finally, the IC might come to value redundancy and competitive analysis, but it will be for naught if the customers of those products—the president and the national security apparatus—don't. Intelligence, for the foreseeable future, will simply take up more of the president's time.[74]

Implications for Intelligence Community Action

Open source versus secret reporting is one way to build redundancy into the intelligence process. It is one powerful form of competitive analysis, but the value of redundancy argues for competitive analysis to be built into every IC product. Among the objections to this strategy is the fact that policy makers, particularly the president, are assumed to have little time for competing and confusing analysis. Thus, internal pressures to "sign on" to intelligence assessment and to declare evidence a "slam dunk" are assumed to help the president. As we have seen, they don't.

For the foreseeable future, U.S. presidents will simply have to spend more time on foreign policy and more time on intelligence. Gone are the naïve days of the 2000 presidential election, when both George Bush and Al Gore spent so much time in classrooms you would have thought they were campaigning for local school board. In our lifetimes at least, the mantle of global leadership will fall on American presidents no matter who they are and no matter their policy.

All presidents and some members of the House and Senate will have to spend less time on some domestic issues, perhaps devolving major responsibility on some issues back down to the states, and more time getting foreign policy right. This is one part of the job of national leaders that, for all practical purposes, can't be learned too much ahead of time. Senators and representatives need to stop rotating off oversight committees and stay there long enough to develop the expertise they need to do the job.

To do that job well they will need more and competing intelligence resources. The President's Daily Brief should regularly contain competitive analysis that the president sees. And the president should see a regular analysis of open source information. Much of the information might be redundant, but that's okay—redundancy is a key aspect of effective knowledge communities.

Job Rotation and Matrix Management Systems

The intelligence community should explore the strategic rotation of employees and matrix management systems.

Knowledge-producing organizations create new knowledge through the "strategic rotation" of their employees. In manufacturing, job rotation has been known to relieve repetitive stress injuries and to contribute modestly to productivity increases.

Companies such as IBM and McDonald's encourage cross-functional job rotations and have found that these rotations help them retain top talent and enrich their products.[75] Strategic rotation is another way of making sure that information is shared widely throughout the company and that employees gain a better understanding of the whole and not just the parts.

In the U.S. government, the most visible and, in some ways, wrenching experiment with strategic rotation has come in the military, as it adapts to the changes required by the passage of the Goldwater-Nichols reforms. In 1986, tired of inter-service competition and the lack of coordination that resulted in some notable military disasters such as the failure to rescue the Iranian hostages, Congress passed legislation that sought to bring about massive cultural change in the military by creating one fighting force out of four.[76] Part and parcel of those changes was the requirement that officers complete a full tour of duty in a joint assignment prior to being selected to the general and flag officer pay grade. "Jointness" is now an accepted part of the military culture.

In an effort to transform the FBI into a more effective counter-terrorist organization, a new career path for special agents was established. This career path gives all agents experience in intelligence collection, analysis, and dissemination, and makes intelligence officer certification a prerequisite for advancement.[77]

In addition to the strategic rotation of employees, companies use matrix management to break down boundaries between divisions and specializations. It is at once a strategy and a culture, as evidenced by an early article on the topic titled "Matrix Management; Not a Structure, a Frame of Mind." In it, the authors caution, "Keeping a company strategically agile while still coordinating its activities across divisions, even continents, means eliminating parochialism, improving communication, and weaving the decision making process into the company's social fabric."[78]

The concept of matrix management is especially important to the intelligence community, where it may not be practical or advisable to make people rotate jobs. After all, the community needs deep technical expertise in things like the interpretation of satellite photography and the construction of small nuclear devices. And it needs deep cultural, social, and language expertise in regions and countries and ethnic conflicts. But what we learned the hard way in the first decade of really trying to deal with transnational threats is that "transnational issues require combinations of regional and functional expertise."[79] In other words, just because a new set of issues is "transnational" doesn't mean that national and regional expertise is irrelevant. In fact, "Terrorism has a base—when you separate it out from its regional base you lose something."[80]

The systematic strategic rotation of analysts with functional expertise into units responsible for regional expertise may be one way to prevent the kinds of mistakes that happened in Iraq when technical expertise was taken out of its political and social context. An internal review of the problems leading up to the incorrect intelligence in Iraq concludes that offices which focus on functional and technical issues have narrowly focused intelligence—and this narrowly focused intelligence needs to be integrated into pieces that are produced by regional or country analytic units.[81] The challenge before the IC is to retain and reward expertise while creating a culture that communicates across divisional lines.

Implications for Intelligence Community Action

Internally, the IC should experiment with both strategic rotation of employees and with matrix management systems. This cannot come at the expense of expertise. But regular participation in cross-functional groupings should be built into the expectations of employees throughout the IC, just as it is built into the expectations of young officers in today's military. These kinds of management strategies should help prevent situations where one form of expertise controls the intelligence product.

Synchrony, Not Sequence

In the intelligence community, actors need to learn to replace sequence with synchrony.

In private sector markets, the modern era has seen "the traditional sequence of research, development, manufacturing, and marketing … replaced by synchrony: specialists from all these functions work together as a team, from the inception of research

to a product's establishment in the market."[82] This change is in response to a much speeded-up world, a world where product cycles dropped from years to months.

The intelligence community is not exempt from this speeded-up product cycle. In the days when the IC watched primarily the Soviet behemoth, the traditional sequence of tasking, collection, analysis, alternative analysis (sometimes), and presentation to the policy maker sufficed. But in a world of "amorphous, continuous threats, for which there may be no 'right time,' " this sequence may need to be replaced with a more synchronous process.[83] Sequential processes worked well when intelligence agencies had to figure out puzzles. It is far less useful in a world of mysteries. In the future it is likely that collectors, analysts, and policy makers will have to work simultaneously in order to understand an emerging surprise.

Implications for Intelligence Community Action

The fast pace of communication in today's world means that sequence is already being replaced by synchrony for policy makers. No wonder the IC often feels like it is, as one consumer put it, "12 hours ahead of CNN." IC products and the consumption of those products need to adapt to the fast pace of the Information Age.

Learning from the Past

The intelligence community needs to be able to learn from the past.

Knowledge-producing organizations view both success and failure systematically and use failure as an opportunity for learning. A study of more than 150 new products concluded that "knowledge gained from failure is often instrumental in achieving subsequent successes.… In the simplest terms, failure is the ultimate teacher."[84] After Boeing introduced two new airplanes that ended up with serious problems, the 737 and 747, the company created "Project Homework." Project Homework looked back at the development of the 737 and 747 and compared that development process to the process used to develop the 707 and the 727—two of the companies' most profitable planes. A set of lessons learned was developed and then applied to other start-ups.

In addition to Boeing, companies like Xerox and British Petroleum have made post-project reviews a regular part of their organizational culture. The result is a culture that values "productive failure as contrasted to unproductive success."[85] Richard Farson and Ralph Keyes show how companies like 3M, Monsanto, and Apple have created breakthroughs by effectively "managing the post-failure era."[86]

Creating this kind of culture in the government has always been difficult, but in an intensely partisan era like today's it is even more difficult. For one thing, the political class to which public sector organizations respond is very reluctant to admit failure of any kind. When admitting failure is unavoidable, as in the case of 9/11 and Iraq, the responsibility for looking at failure tends to be given to outside organizations, who then impose solutions—often through legislation—on the guilty parties. The very people who should be participating in the review of failure—those inside the agencies—are, in the public sector, often kept out of reviews. This results in a defensive crouch on the part of many within the organization and simplistic but important-sounding recommendations. But it does not afford the very people who could benefit from the reviews the opportunity to learn. In the aftermath of the failure to predict the fall of the shah of Iran, all case officers in the country were called home. Some of them waited to be debriefed as to why the agency had missed the signs of the coming revolution. The debriefing never came.[87]

But some parts of the government do, in fact, try to learn from past mistakes. The Army began conducting After Action Reviews in the 1990s. The After Action Review "is a review of training that allows soldiers, leaders, and units to discover for themselves what happened during the training and why…. [They] are not critiques because they do not determine success or failure."[88] The amazing thing about After Action Reviews is that they involve everyone—regardless of rank—and they are structured to discuss leader mistakes. The After Action Reviews mirror the corporate post-failure reviews in their focus on learning from mistakes.

Implications for Intelligence Community Action

The intelligence community needs to be able to learn from its past mistakes, even those that are shrouded in secrecy. Every intelligence failure—large or small—should be followed by an internal, non-punitive review, the purpose of which is to understand where the IC went wrong. This needs to be institutionalized and the people involved in the mistake need to be protected if the mistake was an honest one. Furthermore, the lessons from the mistake have to be shared broadly within the IC and, to the extent possible, with policy makers.

Four decades ago, information about the lack of readiness of the Cuban people to welcome invaders and overthrow Fidel Castro never made it to the president. Three years ago, similar information about the problems likely to be encountered when occupying post-war Iraq appears to have been squelched or ignored or both.

Continuous Innovation

The intelligence community needs to engage in continuous innovation.

In the private sector, the strategies enumerated earlier are used to create organizations capable of continuous innovation—the basic purpose of a knowledge-creating company. Successful 21st century companies have to respond to markets that are global and constantly changing. Thus, they have developed a more holistic approach to management than the companies of the industrial age.

Similarly, 21st century national security threats are global, transnational, and constantly changing. A community built to monitor the Soviet behemoth did not require the constant creation of new knowledge. One very distinguished national security expert summed up the changes as follows: "The notion that I accepted, until recently, that the job of the CIA was to steal secrets, just doesn't match the reality of today—it's a relic of the Cold War…. Intelligence is likely to be less about stealing secrets than telling the decision makers what is really going on."[89] Monitoring the Soviet Union did not require the same degree of constant innovation that continual adaptation to a whole range of state- and non-state-based security threats does. These require a new organizational ethos—one that, hopefully, this report will help the community understand.

Implications for Intelligence Community Action

No government organization is very good at continuous improvement. The obstacles in its way are myriad. But the items offered in this report, if taken together, would go a long way toward creating an organization capable of continuous improvement. Continuous improvement is not simply a cultural attitude but comes from carefully designed systems, systems whose purpose is to create the kind of knowledge that permits change and adaptation.

Recommendations

Building a 21st century intelligence community will take time and a political commitment to reform that lasts even when presidents change and the opposite political party takes over. Many have likened the challenge to the long and difficult process of creating "jointness" in the military—a bipartisan process that took from approximately 1947 to 1986 and beyond. "The intelligence agencies," says former Department of Homeland Security Inspector General Clark Kent Ervin, "are embarking on a similarly long road to reform."[90]

Building a 21st century intelligence capacity will also involve the creation of new and often larger institutions. The United States has never been comfortable with the business of intelligence, but it is time that the country matured into the global leadership role thrust upon it by victory in the Cold War. An effective, global intelligence capacity should not be looked upon as an affirmation of a policy of unilateral action by the political right wing, nor should it be looked upon by the political left wing as a rejection of multi-lateralism. It is simply a fact of life that modern foreign policy makers will need access to a deeper and more robust intelligence capacity than they now have—whether the foreign policy goal is regime change in Iraq or intervention in humanitarian disasters like Darfur.

One place to begin is to study the constructive impact the war colleges have had on military reform. Using that example, a National Intelligence University, similar to the war colleges, should be created. This should be separate from the ongoing work of the IC but responsible for long-term research and development. The CIA has a small internal division responsible for training and for some unclassified outreach, called the Sherman Kent School for Intelligence Analysis. This could be a starting point.

Fundamental reform of the intelligence community is essential to global leadership. We now know, beyond the shadow of a doubt, that we do not know what our national security threats will look like. The solution is to build a different, more comprehensive intelligence community capable of providing its customers knowledge about the threats that this country and the world will face. The following recommendations are intended as a modest first step on that road:

Recommendation 1: The intelligence community should create a National Intelligence University, similar to the military war colleges, to provide continuous education and research to the American intelligence community.

Recommendation 2: The intelligence community should focus the CIA on the collection of secrets and sense making, and create a closer working relationship between collectors and analysts of intelligence as a means of collecting better and more meaningful secrets.

Recommendation 3: The intelligence community should have freer access to information and embed itself in a series of internal government networks. It should standardize security clearances and classification processes within the federal government, and all IT systems should have multi-agency compatibility.

Recommendation 4: The intelligence community should embed itself in a series of external networks including local police, other national governments,

and academic and business circles. This network can be created and managed by the NIC (the National Intelligence Council), which has the advantage of being beholden to no other large bureaucracy or by another entity within the ODNI.

Recommendation 5: The intelligence community should create a purely open source intelligence capacity that has no connection to secret organizations and allow the creation of a purely open source product that is seen by the same policy makers who see the secret products.

Recommendation 6: The intelligence community should experiment with both strategic rotation of employees and with matrix management systems.

Recommendation 7: The intelligence community should institutionalize systematic review of intelligence failures and share widely the knowledge gained.

Recommendation 8: The intelligence community should develop ways of providing intelligence to policy makers in real time.

Endnotes

1. The Counterterrorism Center (CTC) was begun in 1985 and the Counter Narcotics Center (CNC) in 1991.

2. Vice President Al Gore, *Creating a Government that Works Better and Costs Less,* Report of the National Performance Review (Washington, D.C., Government Printing Office, September 7, 1993). Note: The author of this paper was senior policy advisor to Vice President Gore and had as her chief responsibility the creation and management of the National Performance Review.

3. "September 11 and the Adaptation Failure of U.S. Intelligence Agencies," in *International Security,* Vol. 29, Issue #4, Spring 2005, pp. 78–111.

4. Ibid.

5. President Roosevelt fired the Army commander and the Navy commander in charge of Pearl Harbor shortly after the attack and established an investigation into the attack shortly after it happened. In contrast, President Bush awarded the head of the CIA during 9/11 the Congressional Medal of Honor.

6. For a history of the formation of the CIA, see Mark Reibling, Wedge: *From Pearl Harbor to 9/11* (New York, Simon and Schuster, 2004), chapter 4.

7. See Richard A. Best, Jr., "Proposals for Intelligence Reorganization, 1949–2004," CRS Report to Congress, July 29, 2004.

8. As in the case of the new DNI, the statute creating the drug czar sought to invest the office with authority over the budgets of other government entities. In 1997, for the first time in the history of the statute, drug czar Barry McCaffrey (a former four-star general and an extremely competent public servant) exercised a provision in the law that allowed him to refuse to "certify" a line item in the Pentagon's budget. This resulted in a showdown with the secretary of defense and a compromise, brokered by the president, which split the difference. Since the executive branch can send only one budget to Congress at a time, disputes are always likely to be brokered by the president or by OMB. Thus, while giving power to the drug czar to "certify" budgets sounds plausible, the fact that it has been used only once in the 14 years that the drug czar's office has been in effect and the fact that it resulted in an embarrassing news story and the fact that it forced the need for presidential brokering—all mean that it is a power not likely to be used with any frequency.

9. According to Richard Falkenrath, a former official in the Department of Homeland Security: "In short, while reorganizing the intelligence community may ultimately do more good than harm, the history of 9/11 as told by the Commission does not make the case that such a reform is necessary or even necessarily beneficial." "The 9/11 Report, A Review Essay," in *International Security,* Vol. 29, Issue #3, Winter 2004.

10. Pertronius Arbiter, quoted in "Can Spies Be Made Better?" *The Economist,* March 19, 2005, p. 29.

11. Deborah G. Barger, "Toward a Revolution in Intelligence Affairs" (Santa Monica, RAND National Security Research Division, 2005), p. 106.

12. See, for instance, *Harvard Business Review on Knowledge Management* (Boston, Harvard Business School Press, 1998); Carla O'Dell and C. Jackson Grayson, *If Only We Knew What We Know: the Transfer of Internal Knowledge and Best Practice* (New York, Free Press, 1998); Christine Soo, Timothy M. Devinney, David F. Midgley, and Anne Deering, "Knowledge Management, Philosophy, Processes and Pitfalls, in *California Management Review,* July 1, 2002; *Knowledge Management: Four Obstacles to Overcome,* Harvard Management Update Article, Product number U0008B, August 1, 2000; Liam Fahey and Laurence Prusak, "The Eleven Deadliest Sins of Knowledge Management," *California Management Review,* April 1, 1998.

13. Ikujiro Nonaka, "The Knowledge-Creating Company," in *Harvard Business Review on Knowledge Management* (Boston, Harvard Business School Press, 1998), p. 22.

14. Peter F. Drucker, "The Coming of the New Organization," in *Harvard Business Review on Knowledge Management,* p. 3.

15. Conversation with a former intelligence officer, August 11, 2005.

16. Tom Brokaw, "The Long War: The Frightening Evolution of al Qaida, Decentralization has led to deadly staying power," MSNBC.com, June 23, 2005.

17. Author communication with Richard Hunter, GVP and Gartner Fellow, the Gartner Group, July 25, 2005.

18. Marc Sageman writes, "The account of the global Salafi jihad provided so far tries to capture its empirical nature. It is not a specific organization, but a social movement consisting of a set of more or less formal organizations, linked in patterns of interaction ranging from the fairly centralized (the East Africa bombings) to the more decentralized (the two millennial plots) with various degrees of cooperation…. Participants are … linked to each other through complex webs of direct or mediated exchanges." *Understanding Terror Networks* (Philadelphia, University of Pennsylvania Press, 2004), p. 137.

19. See, Eric Lichtblau, "FBI's Translation Backlog Grows," *The New York Times,* July 28, 2005.

20. Communication between the author and James V. Christy II, special agent, Defense Cyber Crime Institute. July 11, 2005.

21. Off-the-record comment of an intelligence officer, April 6, 2005.

22. Joseph A. Horvath, George B. Forsythe, Richard C. Bullis, Patrick J. Sweeny, Wendy Williams, Jeffrey A. McNally, John M. Wattendorf, and Robert J. Sternberg, "Experience, Knowledge and Military Leadership," in T*acit Knowledge in Professional Practice,* edited by Robert J. Sternberg and Joseph A. Horvath (Mahwah, New Jersey, Lawrence Erlbaum Publishers, 1999), p. 44.

23. Peter A. Frensch, "One Concept, Multiple Meanings: On How to Define the Concept of Implicit Learning," in *Handbook of Implicit Learning,* edited by Michael A. Stadler and Peter A. Frensch (Thousand Oaks, California, Sage Publications, 1998), p. 76.

24. Horvath, et al., "Experience, Knowledge and Military Leadership."

25. Ibid., p.55.

26. Gladwell, *Blink* (New York, Little Brown, 2005).

27. Nonaka, "The Knowledge-Creating Company," pp. 21–45.

28. Fahey and Prusak, "The Eleven Deadliest Sins of Knowledge Management."

29. According to one source inside the IC, the CIA had 140,000 applicants in 2004. Conversation with a former intelligence officer, August, 11, 2005.

30. Bruce L. Pechan, "The Collector's Role in Evaluation," in *Inside CIA's Private World, Declassified Articles from the Agency's Internal Journal, 1955–1992,* edited by H. Bradford Westerfield (New Haven, Yale University Press, 1995), p. 103.

31. Ibid.

32. Ibid., p. 105.

33. Communication with Dr. Philip Bobbitt, University of Texas Law School, July 25, 2005.

34. Matthew Brzezinski, "Bust and Boom," *The Washington Post,* December 30, 2001.

35. Melinda Henneberger, "A By-the-Book Officer," *The New York Times,* April 23, 1995.

36. Mark Helm, "Inspectors who caught suspect are honored," Seattle *Post-Intelligencer,* December 21, 1999.

37. Tom Hundley, "Attack was no surprise in London," *Chicago Tribune,* July 10, 2005.

38. William Finnegan, "The Terrorism Beat: How is the NYPD defending the City?," *The New Yorker,* July 25, 2005, p. 58.

39. Communication between the author and Professor Joseph Nye, former director of the National Intelligence Council, April 5, 2005.

40. Nonaka, "The Knowledge-Creating Company," p. 38.

41. Thomas H. Davenport and John Glaser, "Just-in-Time Delivery Comes to Knowledge Management," *Harvard Business Review,* July 1, 2002.

42. Fahey and Prusak, "The Eleven Deadliest Sins of Knowledge Management."

43. *Best Truth, Intelligence in the Information Age* (New Haven, Yale University Press, 2000), p. 151.

44. Anonymous, *Imperial Hubris: Why the West is Losing the War on Terror* (Washington, D.C., Brassey's, 2004), p. 43.

45. Communication with David Ignatius, syndicated columnist for *The Washington Post,* July 25, 2005.

46. Off-the-record comment by an intelligence community official.

47. Private communication with the author, spring 2005.

48. *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington, D.C., Government Printing Office, March 31, 2005), p. 160.

49. Private communication with the author, spring 2005.

50. *The Commission on the Intelligence Capabilities of the United States,* p. 174.

51. Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge, Cambridge University Press, 2001), p. 11.

The following definition has been widely used in discussions of the new strategic world intelligence faces: "A puzzle is a problem for which there is a solution in principle, if only the right information could be found…. A puzzle in intelligence terms is primarily a challenge to collection; the 'counting' issues of the Cold War…. Mysteries are questions without a certain answer, even in principle, because they are future and contingent." Sherman Kent School, Kent Center for Analytic Tradecraft, "Occasional Papers: Making Sense of Transnational Threats," Vol. 3, #1, October 2004, p. 12.

52. B. Hugh Tovar, "The Not-So-Secret War, or How State-CIA Squabbling Hurts U.S. Intelligence," in *Inside CIA's Private World,* p. 192.

53. "How Do We Define Value Chains and Production Networks?" IDS Bulletin, Vol. 32, #3, April 2001, p. 6.

54. See, Elaine C. Kamarck, "The End of Government As We Know It," in John D. Donahue and Joseph S. Nye, Jr., *Market-Based Governance* (Washington, D.C., Brookings, 2002). See also, Stephen Goldsmith and William D. Eggers, *Governing by Network: The New Shape of the Public Sector* (Washington, D.C, Brookings, 2004).

55. Between 1990 and 2000, American political consultants constituted 58% of campaign officials in Latin America, 40% of campaign officials in Eastern Europe, 30% of campaign officials in Western Europe, and 23% of campaign officials in Russia. See, Costas Panagopoulos with Preethi Dayanand, "Pack Your Bags, A Guide to International Political Consulting," *Campaign and Elections Magazine,* April 2005, p. 44.

56. "How to Counter WMD," in *Foreign Affairs,* September/October 2004, p. 85.

57. Officially known as the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, the panel was created by an executive order of President Bush in February, 2004. As part of its mandate, the commission examined the capabilities and challenges of the intelligence community to collect, process, analyze, produce, and disseminate information concerning the capabilities, intentions, and activities of such foreign powers relating to the design, development, manufacture, acquisition, possession, proliferation, transfer, testing, potential or threatened use, or use of Weapons of Mass Destruction, related means of delivery, and other related threats of the 21st century.

58. Open source intelligence includes information on foreign historical, political, economic, social, ideological, cultural, technical, demographic, natural, geographic, and geological data. It is collected from a vast and growing set of publicly available and gray (public, but not widely available) materials, government data, and expert opinion. These sources include web-based materials such as Internet bulletin boards, blogs, and publications, and premium online services; audio/visual materials such as TV/radio broadcasts, public speeches, and unclassified signals; print materials such as books, pamphlets, reports, and magazines; and imagery such as photographs and commercial satellite images.

59. Brian Michael Jenkins, "Intelligence" in Club de Madrid. The International Summit on Democracy and Terrorism: Volume II Confronting Terrorism, pp. 13–19.

60. Communication with the author by Brian Jenkins, October 31, 2003.

61. *The Commission on the Intelligence Capabilities of the United States,* p. 174.

62. Ibid., p. 569.

63. *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York, Henry Holt and Company, 2004).

64. Michael Sulick, "Al Qaeda answers CIA's hiring call," *latimes.com*, July 10, 2005.

65. See Treverton, *Reshaping National Intelligence,* p. 247.

66. Nonaka, "The Knowledge-Creating Company," p. 37.

67. "The Knowing-Doing Gap," November 1999, at gsb_info@gsb.stanford.edu.

68. *The Commission on the Intelligence Capabilities of the United States,* p. 162.

69. Willis C. Armstrong, William Leonhart, William J. McCaffrey, and Herbert C. Rothenberg, "The Hazards of Single-Outcome Forecasting," in *Inside CIA's Private World,* p. 241.

70. "Early Warning Versus Concept," in *Strategic Intelligence: Windows into a Secret World,* edited by Loch K. Johnson and James J. Wirtz (Los Angeles, Roxbury Publishing, 2004) pp. 156–157.

71. Sherman Kent School, "Occasional Papers," p. 2.

72. Walter Pincus, "New Law to Spread the Use of CIA's Analysis Approach," *The Washington Post,* December 20, 2004.

73. Katherine Shraden, "Bush Intelligence Briefing Being Upgraded," *Boston Globe,* July 25, 2005.

74. The downside to this approach, of course, is that it can become a vehicle for alternative policy views, as happened in the Ford administration when the CIA's views of Soviet weakness were challenged. But this is also an argument for non-episodic use of competitive analysis.

75. Gouri Shukla, "Musical Chairs: They're not always as bad as our headline may suggest," *Business Standard,* April 26, 2005.

76. See, James R. Locher III, *Victory on the Potomac* (College Station, Texas, Texas A&M Press, 2002).

77. Congressional Testimony of Robert S. Mueller III, Director, FBI, Before the Senate Committee on Intelligence, February 16, 2005.

78. Christopher A. Bartlett and Sumantra Ghoshal, *Harvard Business Review,* July 1990.

79. Sherman Kent School, "Occasional Papers," p. 10.

80. Interview with a former CIA official, spring 2005.

81. Private communication with the author, spring 2005.

82. Drucker, "The Coming of the New Organization," p. 7.

83. Sherman Kent School, "Occasional Papers," p. 7.

84. David A. Garvin, "Building a Learning Organization," in *Harvard Business Review on Knowledge Management,* p. 61.

85. Ibid., p. 63.

86. Richard Farson and Ralph Keyes, *Whoever Makes the Most Mistakes Wins* (New York, Free Press, 2002).

87. Interview with former DO employee, July 19, 2005.

88. "After Action Reviews," Appendix G to FM 25-101, *Battle Focused Training,* September 30, 1990, at www.au.af.mil/au/awc/awcgate/army/fm25-101.

89. Conversation with a former high-ranking consumer of intelligence, April 7, 2005.

90. Siobhan Gorman, "Overhaul of U.S. Intelligence System May Take 10 years, Analysts Say," *The Baltimore Sun,* July 3, 2005.

ABOUT THE AUTHOR

Elaine C. Kamarck is currently on the faculty of the John F. Kennedy School of Government at Harvard University, where she teaches courses in 21st-century government, innovation in government, public management, and American politics. She joined the Harvard faculty in 1997 as executive director of Visions of Governance for the Twenty-First Century, a new research program at the John F. Kennedy School of Government. In addition, she has served as director of the Innovations in American Government Program, an award program for federal, state, and local governments, and director of a program called "The Future of Public Service." For the past two years, she has worked with the Central Intelligence Agency and the U.S. Department of State on a project titled "Strategic Issues for Intelligence Practice in the 21st Century."

Prior to joining the Harvard faculty, Dr. Kamarck served as senior policy advisor to Vice President Al Gore. She joined the Clinton/Gore administration in March of 1993 and, working directly with Vice President Gore, created the National Performance Review, a White House policy council designed to reinvent government.

Among Dr. Kamarck's most recent publications are "Applying 21st-Century Government to the Challenge of Homeland Security" (IBM Center for The Business of Government, June 2002) and "Government Innovation Around the World." In addition, she publishes frequently in *Newsday* and appears regularly on Fox News discussing American politics.

Dr. Kamarck was educated at Bryn Mawr College and received her Ph.D. in political science from the University of California at Berkeley.

KEY CONTACT INFORMATION

To contact the author:

Elaine C. Kamarck
John F. Kennedy School of Government
Harvard University
79 JFK Street
Cambridge, MA 02138
(617) 495-9002

e-mail: elaine_kamarck@harvard.edu

COLLABORATION: PARTNERSHIPS AND NETWORKS

Leveraging Networks to Meet National Goals: FEMA and the Safe Construction Networks (March 2002)
William L. Waugh, Jr.

Applying 21st-Century Government to the Challenge of Homeland Security (June 2002)
Elaine C. Kamarck

Assessing Partnerships: New Forms of Collaboration (March 2003)
Robert Klitgaard and Gregory F. Treverton

Leveraging Networks: A Guide for Public Managers Working across Organizations (March 2003)
Robert Agranoff

Extraordinary Results on National Goals: Networks and Partnerships in the Bureau of Primary Health Care's 100%/0 Campaign (March 2003)
John Scanlon

Public-Private Strategic Partnerships: The U.S. Postal Service-Federal Express Alliance (May 2003)
Oded Shenkar

The Challenge of Coordinating "Big Science" (July 2003)
W. Henry Lambright

Communities of Practice: A New Tool for Government Managers (November 2003)
William M. Snyder and Xavier de Souza Briggs

Collaboration and Performance Management in Network Settings: Lessons from Three Watershed Governance Efforts (April 2004)
Mark T. Imperial

The Quest to Become "One": An Approach to Internal Collaboration (February 2005)
Russ Linden

Cooperation Between Social Security and Tax Agencies in Europe (April 2005)
Bernhard Zaglmayer, Paul Schoukens, and Danny Pieters

Leveraging Collaborative Networks in Infrequent Emergency Situations (June 2005)
Donald P. Moynihan

E-GOVERNMENT

Supercharging the Employment Agency: An Investigation of the Use of Information and Communication Technology to Improve the Service of State Employment Agencies (December 2000)
Anthony M. Townsend

Assessing a State's Readiness for Global Electronic Commerce: Lessons from the Ohio Experience (January 2001)
J. Pari Sabety and Steven I. Gordon

Privacy Strategies for Electronic Government (January 2001)
Janine S. Hiller and France Bélanger

Commerce Comes to Government on the Desktop: E-Commerce Applications in the Public Sector (February 2001)
Genie N. L. Stowers

The Use of the Internet in Government Service Delivery (February 2001)
Steven Cohen and William Eimicke

State Web Portals: Delivering and Financing E-Service (January 2002)
Diana Burley Gant, Jon P. Gant, and Craig L. Johnson

Internet Voting: Bringing Elections to the Desktop (February 2002)
Robert S. Done

Leveraging Technology in the Service of Diplomacy: Innovation in the Department of State (March 2002)
Barry Fulton

Federal Intranet Work Sites: An Interim Assessment (June 2002)
Julianne G. Mahler and Priscilla M. Regan

The State of Federal Websites: The Pursuit of Excellence (August 2002)
Genie N. L. Stowers

State Government E-Procurement in the Information Age: Issues, Practices, and Trends (September 2002)
M. Jae Moon

Preparing for Wireless and Mobile Technologies in Government (October 2002)
Ai-Mei Chang and P. K. Kannan

Public-Sector Information Security: A Call to Action for Public-Sector CIOs (October 2002, 2nd ed.)
Don Heiman

The Auction Model: How the Public Sector Can Leverage the Power of E-Commerce Through Dynamic Pricing (November 2002, 2nd ed.)
David C. Wyld

The Promise of E-Learning in Africa: The Potential for Public-Private Partnerships (January 2003)
Norman LaRocque and Michael Latham

Digitally Integrating the Government Supply Chain: E-Procurement, E-Finance, and E-Logistics (February 2003)
Jacques S. Gansler, William Lucyshyn, and Kimberly M. Ross

Using Technology to Increase Citizen Participation in Government: The Use of Models and Simulation (April 2003)
John O'Looney

Seaport: Charting a New Course for Professional Services Acquisition for America's Navy (June 2003)
David C. Wyld

E-Reporting: Strengthening Democratic Accountability (February 2004)
Mordecai Lee

Understanding Electronic Signatures: The Key to E-Government (March 2004)
Stephen H. Holden

Measuring the Performance of E-Government (March 2004)
Genie N. L. Stowers

Restoring Trust in Government: The Potential of Digital Citizen Participation (August 2004)
Marc Holzer, James Melitski, Seung-Yong Rho, and Richard Schwester

From E-Government to M-Government? Emerging Practices in the Use of Mobile Technology by State Governments (November 2004)
M. Jae Moon

Government Garage Sales: Online Auctions as Tools for Asset Management (November 2004)
David C. Wyld

Innovation in E-Procurement: The Italian Experience (November 2004)
Mita Marra

Computerisation and E-Government in Social Security: A Comparative International Study (July 2005)
Michael Adler and Paul Henman

The Next Big Election Challenge: Developing Electronic Data Transaction Standards for Election Administration (July 2005)
R. Michael Alvarez and Thad E. Hall

FINANCIAL MANAGEMENT

Credit Scoring and Loan Scoring: Tools for Improved Management of Federal Credit Programs (July 1999)
Thomas H. Stanton

Using Activity-Based Costing to Manage More Effectively (January 2000)
Michael H. Granof, David E. Platt, and Igor Vaysman

Audited Financial Statements: Getting and Sustaining "Clean" Opinions (July 2001)
Douglas A. Brook

An Introduction to Financial Risk Management in Government (August 2001)
Richard J. Buttimer, Jr.

Understanding Federal Asset Management: An Agenda for Reform (July 2003)
Thomas H. Stanton

Efficiency Counts: Developing the Capacity to Manage Costs at Air Force Materiel Command (August 2003)
Michael Barzelay and Fred Thompson

Federal Credit Programs: Managing Risk in the Information Age (April 2005)
Thomas H. Stanton

Grants Management in the 21st Century: Three Innovative Policy Responses (October 2005)
Timothy J. Conlan

HUMAN CAPITAL MANAGEMENT

Profiles in Excellence: Conversations with the Best of America's Career Executive Service (November 1999)
Mark W. Huddleston

Reflections on Mobility: Case Studies of Six Federal Executives (May 2000)
Michael D. Serlin

Managing Telecommuting in the Federal Government: An Interim Report (June 2000)
Gina Vega and Louis Brennan

Using Virtual Teams to Manage Complex Projects: A Case Study of the Radioactive Waste Management Project (August 2000)
Samuel M. DeMarie

A Learning-Based Approach to Leading Change (December 2000)
Barry Sugarman

Labor-Management Partnerships: A New Approach to Collaborative Management (July 2001)
Barry Rubin and Richard Rubin

Winning the Best and Brightest: Increasing the Attraction of Public Service (July 2001)
Carol Chetkovich

A Weapon in the War for Talent: Using Special Authorities to Recruit Crucial Personnel (December 2001)
Hal G. Rainey

A Changing Workforce: Understanding Diversity Programs in the Federal Government (December 2001)
Katherine C. Naff and J. Edward Kellough

Life after Civil Service Reform: The Texas, Georgia, and Florida Experiences (October 2002)
Jonathan Walters

The Defense Leadership and Management Program: Taking Career Development Seriously (December 2002)
Joseph A. Ferrara and Mark C. Rom

The Influence of Organizational Commitment on Officer Retention: A 12-Year Study of U.S. Army Officers (December 2002)
Stephanie C. Payne, Ann H. Huffman, and Trueman R. Tremble, Jr.

Human Capital Reform: 21st Century Requirements for the United States Agency for International Development (March 2003)
Anthony C. E. Quainton and Amanda M. Fulmer

Modernizing Human Resource Management in the Federal Government: The IRS Model (April 2003)
James R. Thompson and Hal G. Rainey

Mediation at Work: Transforming Workplace Conflict at the United States Postal Service (October 2003)
Lisa B. Bingham

Growing Leaders for Public Service (August 2004, 2nd ed.)
Ray Blunt

Pay for Performance: A Guide for Federal Managers (November 2004)
Howard Risher

The Blended Workforce: Maximizing Agility Through Nonstandard Work Arrangements (April 2005)
James R. Thompson and Sharon H. Mastracci

The Transformation of the Government Accountability Office: Using Human Capital to Drive Change (July 2005)
Jonathan Walters and Charles Thompson

INNOVATION

Managing Workfare: The Case of the Work Experience Program in the New York City Parks Department (June 1999)
Steven Cohen

New Tools for Improving Government Regulation: An Assessment of Emissions Trading and Other Market-Based Regulatory Tools (October 1999)
Gary C. Bryner

Religious Organizations, Anti-Poverty Relief, and Charitable Choice: A Feasibility Study of Faith-Based Welfare Reform in Mississippi (November 1999)
John P. Bartkowski and Helen A. Regis

Business Improvement Districts and Innovative Service Delivery (November 1999)
Jerry Mitchell

An Assessment of Brownfield Redevelopment Policies: The Michigan Experience (November 1999)
Richard C. Hula

San Diego County's Innovation Program: Using Competition and a Whole Lot More to Improve Public Services (January 2000)
William B. Eimicke

Innovation in the Administration of Public Airports (March 2000)
Scott E. Tarry

Entrepreneurial Government: Bureaucrats as Businesspeople (May 2000)
Anne Laurent

Rethinking U.S. Environmental Protection Policy: Management Challenges for a New Administration (November 2000)
Dennis A. Rondinelli

The Challenge of Innovating in Government (February 2001)
Sandford Borins

Understanding Innovation: What Inspires It? What Makes It Successful? (December 2001)
Jonathan Walters

Government Management of Information Mega-Technology: Lessons from the Internal Revenue Service's Tax Systems Modernization (March 2002)
Barry Bozeman

Advancing High End Computing: Linking to National Goals (September 2003)
Juan D. Rogers and Barry Bozeman

MANAGING FOR PERFORMANCE AND RESULTS

Corporate Strategic Planning in Government: Lessons from the United States Air Force (November 2000)
Colin Campbell

Using Evaluation to Support Performance Management: A Guide for Federal Executives (January 2001)
Kathryn Newcomer and Mary Ann Scheirer

Managing for Outcomes: Milestone Contracting in Oklahoma (January 2001)
Peter Frumkin

The Challenge of Developing Cross-Agency Measures: A Case Study of the Office of National Drug Control Policy (August 2001)
Patrick J. Murphy and John Carnevale

The Potential of the Government Performance and Results Act as a Tool to Manage Third-Party Government (August 2001)
David G. Frederickson

Using Performance Data for Accountability: The New York City Police Department's CompStat Model of Police Management (August 2001)
Paul E. O'Connell

Moving Toward More Capable Government: A Guide to Organizational Design (June 2002)
Thomas H. Stanton

The Baltimore CitiStat Program: Performance and Accountability (May 2003)
Lenneal J. Henderson

Strategies for Using State Information: Measuring and Improving Program Performance (December 2003)
Shelley H. Metzenbaum

Linking Performance and Budgeting: Opportunities in the Federal Budget Process (January 2004, 2nd ed.)
Philip G. Joyce

How Federal Programs Use Outcome Information: Opportunities for Federal Managers (February 2004, 2nd ed.)
Harry P. Hatry, Elaine Morley, Shelli B. Rossman, and Joseph S. Wholey

Performance Leadership: 11 Better Practices That Can Ratchet Up Performance (May 2004)
Robert D. Behn

Performance Management for Career Executives: A "Start Where You Are, Use What You Have" Guide (October 2004, 2nd ed.)
Chris Wye

Staying the Course: The Use of Performance Measurement in State Governments (November 2004)
Julia Melkers and Katherine Willoughby

MARKET-BASED GOVERNMENT

Determining a Level Playing Field for Public-Private Competition (November 1999)
Lawrence L. Martin

Implementing State Contracts for Social Services: An Assessment of the Kansas Experience (May 2000)
Jocelyn M. Johnston and Barbara S. Romzek

A Vision of the Government as a World-Class Buyer: Major Procurement Issues for the Coming Decade (January 2002)
Jacques S. Gansler

Contracting for the 21st Century: A Partnership Model (January 2002)
Wendell C. Lawther

Franchise Funds in the Federal Government: Ending the Monopoly in Service Provision (February 2002)
John J. Callahan

Making Performance-Based Contracting Perform: What the Federal Government Can Learn from State and Local Governments (November 2002, 2nd ed.)
Lawrence L. Martin

Moving to Public-Private Partnerships: Learning from Experience around the World (February 2003)
Trefor P. Williams

IT Outsourcing: A Primer for Public Managers (February 2003)
Yu-Che Chen and James Perry

The Procurement Partnership Model: Moving to a Team-Based Approach (February 2003)
Kathryn G. Denhardt

Moving Toward Market-Based Government: The Changing Role of Government as the Provider (March 2004, 2nd ed.)
Jacques S. Gansler

Transborder Service Systems: Pathways for Innovation or Threats to Accountability? (March 2004)
Alasdair Roberts

Competitive Sourcing: What Happens to Federal Employees? (October 2004)
Jacques S. Gansler and William Lucyshyn

Implementing Alternative Sourcing Strategies: Four Case Studies (October 2004)
Edited by Jacques S. Gansler and William Lucyshyn

Designing Competitive Bidding for Medicare (November 2004)
John Cawley and Andrew B. Whitford

International Experience Using Outsourcing, Public-Private Partnerships, and Vouchers (October 2005)
Jón R. Blöndal

TRANSFORMATION OF ORGANIZATIONS

The Importance of Leadership: The Role of School Principals (September 1999)
Paul Teske and Mark Schneider

Leadership for Change: Case Studies in American Local Government (September 1999)
Robert B. Denhardt and Janet Vinzant Denhardt

Managing Decentralized Departments: The Case of the U.S. Department of Health and Human Services (October 1999)
Beryl A. Radin

Transforming Government: The Renewal and Revitalization of the Federal Emergency Management Agency (April 2000)
R. Steven Daniels and Carolyn L. Clark-Daniels

Transforming Government: Creating the New Defense Procurement System (April 2000)
Kimberly A. Harokopus

Trans-Atlantic Experiences in Health Reform: The United Kingdom's National Health Service and the United States Veterans Health Administration (May 2000)
Marilyn A. DeLuca

Transforming Government: The Revitalization of the Veterans Health Administration (June 2000)
Gary J. Young

The Challenge of Managing Across Boundaries: The Case of the Office of the Secretary in the U.S. Department of Health and Human Services (November 2000)
Beryl A. Radin

Creating a Culture of Innovation: 10 Lessons from America's Best Run City (January 2001)
Janet Vinzant Denhardt and Robert B. Denhardt

Transforming Government: Dan Goldin and the Remaking of NASA (March 2001)
W. Henry Lambright

Managing Across Boundaries: A Case Study of Dr. Helene Gayle and the AIDS Epidemic (January 2002)
Norma M. Riccucci

Managing "Big Science": A Case Study of the Human Genome Project (March 2002)
W. Henry Lambright

The Power of Frontline Workers in Transforming Government: The Upstate New York Veterans Healthcare Network (April 2003)
Timothy J. Hoff

Making Public Sector Mergers Work: Lessons Learned (August 2003)
Peter Frumkin

Efficiency Counts: Developing the Capacity to Manage Costs at Air Force Materiel Command (August 2003)
Michael Barzelay and Fred Thompson

Managing the New Multipurpose, Multidiscipline University Research Centers: Institutional Innovation in the Academic Community (November 2003)
Barry Bozeman and P. Craig Boardman

The Transformation of the Government Accountability Office: Using Human Capital to Drive Change (July 2005)
Jonathan Walters and Charles Thompson

Executive Response to Changing Fortune: Sean O'Keefe as NASA Administrator (October 2005)
W. Henry Lambright

Transforming the Intelligence Community: Improving the Collection and Management of Information (October 2005)
Elaine C. Kamarck

2004 PRESIDENTIAL TRANSITION SERIES

Government Reorganization: Strategies and Tools to Get It Done (August 2004)
Hannah Sistare

Performance Management for Political Executives: A "Start Where You Are, Use What You Have" Guide (October 2004)
Chris Wye

Becoming an Effective Political Executive: 7 Lessons from Experienced Appointees (January 2005, 2nd ed.)
Judith E. Michaels

Getting to Know You: Rules of Engagement for Political Appointees and Career Executives (January 2005)
Joseph A. Ferrara and Lynn C. Ross

SPECIAL REPORTS

Enhancing Security Throughout the Supply Chain (April 2004)
David J. Closs and Edmund F. McGarrell

Assessing the Impact of IT-Driven Education in K–12 Schools (May 2005)
Ganesh D. Bhatt

Investing in Supply Chain Security: Collateral Benefits (May 2005)
James B. Rice, Jr., and Philip W. Spayd

CENTER FOR HEALTHCARE MANAGEMENT REPORTS

The Power of Frontline Workers in Transforming Healthcare Organizations: The Upstate New York Veterans Healthcare Network (December 2003)
Timothy J. Hoff

IT Outsourcing: A Primer for Healthcare Managers (December 2003)
Yu-Che Chen and James Perry

BOOKS*

Collaboration: Using Networks and Partnerships
(Rowman & Littlefield Publishers, Inc., 2004)
John M. Kamensky and Thomas J. Burlin, editors

E-Government 2001
(Rowman & Littlefield Publishers, Inc., 2001)
Mark A. Abramson and Grady E. Means, editors

E-Government 2003
(Rowman & Littlefield Publishers, Inc., 2002)
Mark A. Abramson and Therese L. Morin, editors

Human Capital 2002
(Rowman & Littlefield Publishers, Inc., 2002)
Mark A. Abramson and Nicole Willenz Gardner, editors

Human Capital 2004
(Rowman & Littlefield Publishers, Inc., 2004)
Jonathan D. Breul and Nicole Willenz Gardner, editors

Innovation
(Rowman & Littlefield Publishers, Inc., 2002)
Mark A. Abramson and Ian Littman, editors

Leaders
(Rowman & Littlefield Publishers, Inc., 2002)
Mark A. Abramson and Kevin M. Bacon, editors

Learning the Ropes: Insights for Political Appointees
(Rowman & Littlefield Publishers, Inc., 2005)
Mark A. Abramson and Paul R. Lawrence, editors

Managing for Results 2002
(Rowman & Littlefield Publishers, Inc., 2001)
Mark A. Abramson and John M. Kamensky, editors

Managing for Results 2005
(Rowman & Littlefield Publishers, Inc., 2004)
John M. Kamensky and Albert Morales, editors

Memos to the President: Management Advice from the Nation's Top Public Administrators
(Rowman & Littlefield Publishers, Inc., 2001)
Mark A. Abramson, editor

New Ways of Doing Business
(Rowman & Littlefield Publishers, Inc., 2003)
Mark A. Abramson and Ann M. Kieffaber, editors

The Procurement Revolution
(Rowman & Littlefield Publishers, Inc., 2003)
Mark A. Abramson and Roland S. Harris III, editors

Transforming Government Supply Chain Management
(Rowman & Littlefield Publishers, Inc., 2003)
Jacques S. Gansler and Robert E. Luby, Jr., editors

Transforming Organizations
(Rowman & Littlefield Publishers, Inc., 2001)
Mark A. Abramson and Paul R. Lawrence, editors

* Available at bookstores, online booksellers, and from the publisher (www.rowmanlittlefield.com or 800-462-6420).

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion on new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

The Center is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Center focuses on the future of the operation and management of the public sector.

About IBM Business Consulting Services

With consultants and professional staff in more than 160 countries globally, IBM Business Consulting Services is the world's largest consulting services organization. IBM Business Consulting Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line business value. For more information visit www.ibm.com/bcs.

For additional information, contact:
Mark A. Abramson
Executive Director
IBM Center for The Business of Government
1301 K Street, NW
Fourth Floor, West Tower
Washington, DC 20005
(202) 515-4504, fax: (202) 515-4375

e-mail: businessofgovernment@us.ibm.com
website: www.businessofgovernment.org