Better Ways to Fix U.S. Intelligence

by Bruce Berkowitz

Many experts, both inside and outside government, are beginning to agree on the necessary features of a modern, effective intelligence organization. Unfortunately, practice is lagging theory. Despite the apparent consensus on the need for change, recent intelligence failures suggest that U.S. intelligence has yet to leave its Cold War–era methods and structure behind. All of this raises the questions of why it has been so hard to modernize American intelligence and what practical steps could ensure that needed reforms finally take hold.

The Basics of Better Intelligence

Anyone who reads government reports and scholarly studies about intelligence will find a consensus emerging about how to produce effective intelligence in the post–Cold War, information-age environment. It is generally agreed that, first, an intelligence service needs to have a wide field of vision, because threats today can arise suddenly and from many sources. Intelligence organizations must be able to detect threats as diverse as terrorism in the Middle East, organized crime in Russia, and a financial crisis in Latin America. Because organizations, like human beings, have trouble focusing on several issues at once, intelligence officials have to create rules and incentives that lead intelligence personnel to monitor multiple information sources and make sure that information reaches the people who need it.

Secondly, modern intelligence organizations must have agility and flexibility. Because today's threats can take so many forms, U.S. intelligence must be able to assemble whatever expertise it requires for a mission into an effective, integrated team. One problem may require engineers who understand ballistic missile systems developed in North Korea; another could call

Bruce Berkowitz is a research fellow at the Hoover Institution and a contributing editor to *Orbis*.

for medical and social science experts who understand Africa's AIDS epidemic and its potential effects on the stability of South Africa and Botswana.

The third capability needed is efficiency and focus. Intelligence spending fell in the early 1990s and has remained essentially flat even as the demand for intelligence has grown. This has made finding the most efficient solution to an intelligence problem more important than ever. The private sector, which has more capital, more people, and greater flexibility than government, is a vital partner. The intelligence community must use unclassified information and expertise from commercial and other nongovernmental sources whenever it can. Intelligence managers must then concentrate scarce government funds on those tasks that the private sector cannot (or should not) perform.

To make sure that information does not get lost in the system or slip between the cracks, the fourth requirement is for multiple lines of communication connecting people who have information with people who need it. Intelligence organizations must have as few choke points as possible. Dependence on the success of a particular organization, system, program, or official can lead to what an engineer would call a "single-point failure"—the breakdown of the entire intelligence process because one key link did not perform correctly.

The fifth and final requirement, according to the consensus view, is for direct interaction and transparency. Intelligence consumers (like most people today) expect greater insight into the information they receive. They are unwilling to accept judgments at face value, even from recognized authorities, and want to know where uncertainty in an analysis lies. To gain this sort of insight, they want more interaction with intelligence producers. They also want products that are tailored to their specific needs. If intelligence organizations do not meet these expectations, their products will be ineffective or ignored.

In the business world and think tanks, organization theorists had long talked about networked organizations. It was a simple matter to apply the same principles to intelligence, and articles describing this kind of intelligence community began to appear in the mid-1990s.[1] Several efforts to develop this approach also arose within the intelligence community itself, with some significant results. In the early 1990s, for example, the CIA introduced electronic mail and Lotus Notes into its operations. The latter did not, like true network technology, enable groups of people to communicate directly with each other, but it did allow several people to work on a single document simultaneously. In 1995, the intelligence community began operating Intelink, a Mosaic-based intranet enabling any organization that was a member of the network to deliver electronic documents (including images)

[1] See, for example, Bruce Berkowitz, "Information Age Intelligence," *Foreign Policy*, Summer 1996, pp. 35–50; and Berkowitz, "Technology and Intelligence Reform," *Orbis,* Winter 1997, pp. 107–19.

directly to any other member. The following year, the CIA's deputy director for intelligence issued a strategic plan with the ambitious goal of improving the communications and data processing systems available to the typical analyst. The plan envisioned ad hoc, virtual teams of analysts that could draw on whatever expertise was required to address problems as they appeared.[2] In 1997, the CIA's deputy director for science and technology circulated a monograph describing an "agile intelligence enterprise" that would be able to divide itself along functional, geographic, and technological lines and would use new network technologies to assemble teams tailored to particular problems.[3] The emphasis on technology-assisted networks has been echoed more recently in a vision statement from the director of central intelligence, as well as in the statements and writings of other public officials and scholars of intelligence policy.[4]

Recent Failures

Unfortunately, although a common vision for U.S. intelligence may be emerging, the intelligence community is having difficulty bringing it to fruition—as recent intelligence failures demonstrate. American intelligence failed to anticipate the March 1995 sarin gas attack by the Aum Shinrikyo cult on the Tokyo subway system, the 1997–98 economic crises in Asia and Russia, India's May 1998 nuclear weapons tests, and North Korea's 1999 ballistic missile test. It provided no warning prior to terrorist strikes on U.S. embassies and military personnel in Africa and Saudi Arabia, mistakenly targeted the Chinese embassy in Belgrade during Operation Allied Force in 1999, and apparently misidentified the al-Shifa pharmaceutical plant in Sudan in August 1998. To be fair, failures are inevitable in the intelligence business. What is especially troubling, however, is the *nature* of these failures, which clearly reveal organizational rigidity, poor planning, insufficient use of outside resources, and isolation of intelligence providers and consumers.

The most recent failure, the bombing of the destroyer USS *Cole* in Yemen in October 2000, provides some of the most vivid evidence of the problems. Many signs suggested that hostility toward the United States was growing throughout the Arab world during the summer and fall of 2000. At

[2] Directorate of Intelligence, *Analysis: Directorate of Intelligence in the 21st Century* (Washington, D.C.: Central Intelligence Agency, 1996).

[3] Ruth A. David, "The Agile Intelligence Enterprise: Enhancing Speed, Flexibility, and Capacity through Collaborative Operations," draft memo, Directorate of Science and Technology, Central Intelligence Agency, Summer 1997.

[4] See, for example, "DCI's Strategic Intent," cited in *Director of Central Intelligence Annual Report for the United States Intelligence Community* (Washington, D.C.: Central Intelligence Agency, May 1999); Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World* (Fairfax, Va.: AFCEA International Press, 2000); and Gregory W. Treverton, *Reshaping National Intelligence for an Age of Information* (New York: Cambridge University Press, 2001).

least one intelligence report issued in the month preceding the bombing had apparently raised the possibility that terrorists would attack a U.S. warship somewhere in the Middle East.[5] Indeed, the director of central intelligence was sufficiently concerned about the potential threat that he warned President Clinton against vetoing a U.N. resolution condemning Israel, lest this trigger an attack on the United States.[6]

Despite these developments, the *Cole* was sent to Aden harbor for refueling while en route to the Persian Gulf. Although Yemen had been a center of terrorist activity for many years, the Yemeni government and the United States had recently tried to improve relations. Port calls by U.S. warships were part of this effort. On the morning of October 19, a small boat loaded with explosives pulled alongside the destroyer, which had been at a relatively low state of alert, and detonated, killing seventeen sailors and wounding thirty-nine. After the attack, U.S. Navy and Defense Department investigators concluded that, despite the various warning signs, no single piece of advance information had been specific enough to lead the commander of the *Cole* to take extraordinary precautions.[7]

The problem in this incident was in the effective flow and use of information—the essential feature of a modern intelligence organization. Indeed, the intelligence community failed in each of the dimensions experts agree are critical to effective intelligence today. Specifically, intelligence organizations were so focused on the threat of violence in the immediate vicinity of Israel that they missed indicators in more distant, less obvious regions such as Yemen. They failed to integrate classified information that warned of danger to U.S. personnel with unclassified information (such as the television broadcasts by lieutenants of Osama bin Laden) that might have provided a broader picture of the potential threat. Choke points prevented information that was available to some organizations (embassies) from reaching others (U.S. military commands and the destroyer itself). The warning system on which the *Cole* depended appears to have lacked redundancy, as it was critically dependent on Central Command. Lastly, the captain of the *Cole* had only limited interaction with intelligence producers and thus lacked a full appreciation of the context. Had he been aware of the low-level hostility in Yemen, the increasing tension throughout the Arab world, and other,

[5] Mark Hosenball and Greg Vistica, "The Search for Clues: Did Officials Miss Hints of an Impending Attack?" *Newsweek*, Nov. 6, 2000.

[6] See Steven Lee Myers, "U.S. Officials Tell of Getting Warning Last Month, But Say It Was Too Vague," *New York Times*, Oct. 14, 2000; and Bill Gertz, "NSA's Warning Arrived Too Late to Save the *Cole*," *Washington Times*, Oct. 25, 2000.

[7] See U.S. Department of Defense, "Navy Announces Results of Its Investigation on *USS Cole*," press release, Jan. 19, 2001; Department of Defense, *DoD USS Cole Commission Report* (Washington, D.C.: Department of Defense, Jan. 9, 2001); and Steven Lee Myers, "After Cole's Bombing, Pentagon Finds Ongoing Lapses in Gulf Security," *New York Times*, Jan. 1, 2001.

almost subliminal factors, he might have put his crew on a higher level of alert.

Perhaps, as the investigators found, no single warning sign was sufficient to cause a responsible official to trigger a general alert. But that is exactly the point. Systems should not depend on whether a precisely defined piece of information reaches a specifically designated gatekeeper. One would refer to the kind of amorphous warning signs that existed prior to the attack on the *Cole* as "buzz," that is, subtle and not-so-subtle indicators that rattle around in a network. In the everyday world, buzz raises the average person's overall level of awareness. People talk to each other and share news, insights, and impressions. This is how networks work. Instead of centralized control of some sort, individual connections and decisions determine the flow of information.

In the future, the United States will likely face the kinds of threats that generate such buzz, as opposed to those involving a single "tripwire" event that by itself sends a clear signal of danger. This is one reason why networks are better suited to addressing diffuse threats. Because networked organizations do not depend on the omniscience of a single director, they are often better able to look in many directions at once. Networked organizations are less likely to suffer a single-point failure caused by a faulty decision or a lapse of judgment by one official at a critical position in a chain of command. Intelligence organizations need this kind of resilience in order to function effectively.

Networked organizations are better able to look in many directions at once.

Some of the other failures of the past several years might also have been avoided if U.S. intelligence had been more agile and better networked. For example, U.S. intelligence might have anticipated the Indian nuclear test if it had been able to cast for a wider range of expert opinion. Many India watchers outside the U.S. government were sure that the governing Bharatiya Janata Party would fulfill its promise to resume testing. Moreover, if intelligence producers had been able to circumvent top officials in the Clinton administration (who were preoccupied with domestic affairs and scandal in early 1999) and deal directly with members of Congress concerned with proliferation, they might have raised the visibility of the Indian situation. Similarly, a process that was open to outside sources of information might have avoided the apparently mistaken targeting of the al-Shifa pharmaceutical plant in Sudan.

Impediments to Change

These recent failures raise a troubling question. If experts understand the kind of intelligence organization that is required to cover today's diffuse, highly varied threats, what is preventing U.S. intelligence from reforming accordingly? One problem is that, even as reformers try to bring in the new model of intelligence through the front door, they reintroduce the old model through the back door. The new model of intelligence, namely, networks and adaptable organizations, is incompatible with traditional notions about how intelligence organizations are supposed to operate. Modern organizational concepts are especially at odds with long-held beliefs about intelligence production, security, and planning. This dogma has repeatedly thwarted reform, often without reformers' being aware of what they were challenging.

The traditional model of intelligence is actually a variant of the classic model of a bureaucratic organization. A bureaucracy has three defining features: a division of labor, a hierarchical structure and chain of command, and standard operating procedures that are often (but not always) formally codified. Although bureaucracies have a checkered reputation (after all, the phrase "Washington bureaucrat" is almost always intended as an epithet), they are not necessarily bad. Indeed, bureaucracy may be one of the great management inventions of all time. Compared to some earlier forms of organization (e.g., hordes and mobs), bureaucracies are more efficient and have better accountability. Bureaucracies allow specialization and clear lines of communication and control.[8] A bureaucratic intelligence organization was perfect for monitoring the Soviet threat largely because the Soviet Union was itself an incorrigibly bureaucratic system. It was possible to assign an analyst, department, or agency to monitor some aspect of the Soviet threat for years. The Soviets changed incrementally, and so did the intelligence community.

A traditional bureaucracy is ill suited for today's more numerous and less predictable threats, however. For example, consider how a bureaucracy assigns responsibilities. Lower-level officials get their assignments from higher-level officials; lower-level departments get their assignments from higher-level departments. If no one is explicitly assigned responsibility for monitoring a particular threat, it is likely to be ignored. Effective bureaucrats shun responsibilities that do not fit into their formally defined assignment. They also draw criticism if they do not focus on their own duties or, even worse, divert their attention to someone else's turf.

This kind of specialization is one of the features that make bureaucracies so efficient,[9] but it also reduces the base from which a bureaucracy can draw new ideas and information. Even worse, these traits make traditional intelligence organizations critically dependent on whether supervisory officials correctly anticipate threats. The result is a chicken-and-egg problem. Intelligence agencies will not monitor a threat until higher-level officials tell

[8] For an insightful analysis of alternative forms of organization and their evolution in a military context, see the recent study by John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, Calif.: RAND, 2000).

[9] See Max Weber, *The Theory of Social and Economic Organization* (New York: Oxford University Press, 1947). Also see Anthony Downs, *Inside Bureaucracy* (Boston: Little, Brown, 1967).

them to do so, but higher-level officials cannot tell them to monitor a threat until they are aware of its importance. This is an oversimplification, of course. Most intelligence managers do not merely follow their noses like a horse with blinders. Nevertheless, the essential truth is that intelligence officials justify their programs according to established priorities. Those programs that cannot show how they address a high-priority requirement are the first to face the budget ax. The same is true in the allocation of existing assets. Any operation that is not, in official policy, a high priority will be last in line for access to collection systems and analytic support.

It is in precisely such circumstances that intelligence fails. Investigation of the failure to detect India's nuclear test showed, for example, that some assets that might have detected Indian preparations were unavailable because they were covering other targets—Iraq and North Korea, for example—that had a higher priority under the planning policies of the time. By the time a bureaucratic organization can perceive a threat and develop plans and policies to address it, it may be too late.

Similarly, a traditional bureaucracy is ill suited for using modern information technology, especially networked communications. In an open-architecture, networked organization, the number of opportunities for providing, supplying, or sharing information—and, thus, the power of the network—increases exponentially as each new member joins.[10] Yet a bureaucracy's traditional chain of command, lines of authority, and mission responsibilities are all aimed at channeling and limiting the opportunities of organization members to interact with each other and with outsiders. A bureaucratic intelligence agency, in other words, erects its own barriers to the information revolution.

Breaking the Traditional Model

The challenge of intelligence reform is therefore not how to make the intelligence bureaucracy work better, but rather how to make the intelligence community operate less like a bureaucracy. The measures required to achieve this bear little resemblance to traditional intelligence reforms, but could have a much greater effect on how the intelligence community operates. Most fit into the three broad categories listed below.

1. *Measures that break down hierarchies and stovepipes*. Such organizational barriers restrict the flow of information, impede interaction among intelligence specialists, and inhibit exchanges between the intelligence community and the outside world. In practice, changing the structure entails, first, reducing the separation between analysts and consumers. The traditional

[10] This phenomenon is often referred to as "Metcalfe's Law," after Robert Metcalfe, the inventor of Ethernet, one of the early networking protocols that made the internet possible.

intelligence model kept analysts apart from consumers to ensure objectivity and avoid politicization. (It also reflected an ivory-tower mentality.) Modern information consumers want direct contact with producers and assume that analysts will maintain their objectivity. The intelligence community has in fact tried recently to bridge the gap by holding briefings for intelligence users and sending analysts to work directly with their consumers. Even so, most analysts still remain separated from intelligence users both organizationally and geographically. Analysts need to be encouraged to get out of their offices, know their customers, and "sell" their products. To promote the new approach, intelligence officials could make serving a stint among consumers a prerequisite for promotion, or agencies could offer bonuses to those analysts who take on such assignments.

Intelligence organizations must also allow analysts to speak for themselves. The traditional intelligence model assumes that internal coordination improves the product and protects an agency's "brand name." Unfortunately, coordination also creates choke points that prevent analysts and consumers from speaking with each other. In this regard, intelligence agencies could learn from the private sector. Investment banks do not make their economists coordinate forecasts or their equity analysts coordinate company assessments. Law firms do not require partners to get approval for arguments they make in court. In each case, the assumption is that, having reached a certain level of seniority, professionals have proved their ability. Quality assurance focuses on hiring and promotion, not on products. Intelligence organizations can do the same. Instead of trying to guarantee that each product is perfect, they should ensure that any analyst in the intelligence community has met certain standards and can speak as an authority. Peer review, especially on matters that depend on judgment more than fact, is much overrated.[11]

Removing structural barriers also requires developing alternative approaches to security. Traditionally, protecting secrets has demanded rigid, hierarchical bureaucracies. Organizations identify classes of information that are supposed to be secret, classes of people who are supposed to have access to the information, and standard operating procedures that define how the people are to handle the information. Such an approach lacks the flexibility required to adapt to rapid changes in user requirements and modern technology. Intelligence personnel certified as responsible and loyal should be given greater personal responsibility for protecting secrets. Professional standards of conduct should be at least as important as formal regulations. Developing one's own secure "information space" should become a part of the intelligence tradecraft. Security officials should act less like police who enforce rules (often in an adversarial manner) and more like specialized support staff who assist intelligence personnel in doing their jobs in a secure

[11] This article was not peer reviewed.

fashion. Technology could play a role here, too, by enabling intelligence personnel to detect when they are being monitored, to encrypt digital data more easily, and to take other security precautions.

2. *Measures that make the intelligence community perform more like a market.* The intelligence community must become more efficient, and spending decisions should more closely reflect actual demand. In addition, the measures proposed here would also promote competition among producers by encouraging intelligence users to find alternative sources of information.

An important part of this shift is to calculate the true costs of intelligence products. Incredible as it may seem, it would be hard for any official at the National Reconnaissance Office (NRO) to tell you how much a specific satellite image cost, or for a CIA official to quote a cost estimate for an intelligence assessment. You could, however, probably learn the cost of an entire satellite *program* or the annual budget of the Directorate of Intelligence. Knowing true costs of products and services and allowing supply and demand to set prices are fundamental components of efficient markets. Officials often explain that it is too hard to estimate the cost of an intelligence product because U.S. intelligence programs are too large and complex. But private sector organizations do this all the time—even large, complex organizations. General Motors knows the unit cost of its automobiles to the dollar. DRI, Accenture, and other consulting firms can tell you the exact cost of one of their analytic reports. Johnnie Cochran can give you a breakdown, hour by hour, lawyer by lawyer, of how much it cost to defend O. J. Simpson (as could, of course, Simpson himself, who presumably got an itemized bill). Instead of pricing goods and services, intelligence officials put all their resources into a big pot and try to allocate them using a complex system of requirements and priorities, much like the process the Soviet Union used to plan its economy. The results, in both cases, speak for themselves.

Once costs have been determined, the intelligence community should also charge for its products. If intelligence products and services have specific prices, intelligence consumers can make purchasing decisions according to their own priorities. This would have the added benefit of forcing political leaders to make explicit decisions about which agencies would receive funding for intelligence support and which would do without. Currently, a politician can point to press reports citing the NRO's budget and ask why, if the United States spends approximately $6 billion per year on intelligence satellites, a particular user did not receive an image he needed. That question will seem reasonable as long as costs, prices, and allowances are unknown, because intelligence will always be perceived as an endless resource—when nothing could be further from the truth. Top intelligence officials should keep a funding reserve for long-range requirements that are so detached from the day-to-day needs of intelligence users that market-based management would be unable to guarantee their funding. But most programs would likely benefit from such an approach.

Another market-oriented measure would be to lower barriers to lateral entry of personnel. In the current system, most senior and middle-level intelligence analysts and case officers begin their careers at a junior level and rise through their respective organizations. The recruitment process, especially the difficulty of obtaining a security clearance, discourages people with established careers in other fields from considering working in intelligence. Streamlining this process requires spending more money and changing attitudes about how one becomes an intelligence officer, or even what being a “real” intelligence officer is. This suggestion may seem incidental to the substance of intelligence, but imagine the impact on the intelligence community if the process of getting a job at the CIA, Defense Intelligence Agency, or National Security Agency (NSA) required no more time, uncertainty, or hassle than getting a job at IBM, General Electric, or Oracle. Barriers to lateral entry insulate intelligence agencies from outside expertise and ideas. Lowering these barriers will inject new thinking into intelligence organizations.

3. *Measures that exploit new technology.* Technology is not a cure-all, but certain key investments in technology could further reduce organizational barriers and make intelligence organizations more agile. For example, user-friendly tools could assist all-source analysts in using specialized information. The information revolution is increasing not only the volume, but also the complexity of data. Analysts need to be able to use this information effectively and present it to intelligence consumers in an understandable form. Moreover, analysts need tools so that even generalists without in-depth scientific training can use technical data easily (e.g., software that can scan a digital image to seek out the particular electronic signature of a truck or missile launcher and superimpose its location on a conventional map). More importantly, by making it possible for the average analyst to use these kinds of data, analysts will likely find new and unexpected applications for data and new ways to solve long-standing intelligence problems.

One of the greatest needs, with regard to technology, is for communications and software standards. Incompatibilities between information systems are as effective as rules and culture in reinforcing organizational barriers. Until interoperability improves, individuals within the intelligence community will continue to find it difficult to communicate and collaborate, defeating any attempt to take advantage of networks.

Improving communications capacity, or bandwidth, is also crucial to countering the data glut intelligence analysts face. The situation is only likely to get worse in the face of increasing interaction among producers and users of intelligence, the sharing of ever-larger data sets, and an expanding base of users and information sources. Communication links will themselves become a major constraint on change within the intelligence community. Investments in communications capacity may seem more like a logistical detail than a major policy reform, but they are utterly essential to improving intelligence operations.

Effective intelligence reform in the contemporary context will likely be less dramatic than the creation of the intelligence community fifty years ago. No major new organization will suddenly spring to life, as the CIA and NSA did in the late 1940s. Yet measures such as those proposed here could be just as challenging to implement. Most will pose major changes in the intelligence community's organizational culture. Experience suggests that such changes are the most difficult of all—but also the most effective and most significant.