Policy Analysis

No. 439 May 16, 2002

Building Leverage in the Long War

Ensuring Intelligence Community Creativity in the Fight against Terrorism

by James W. Harris

Executive Summary

Intelligence is often cited as a critical element in the war against terrorism and, indeed, it is. The U.S. intelligence community has a golden opportunity to develop the capabilities that will make a decisive difference in a war that may last a generation or more. The adversary will not disappear as the campaign to root the al-Qaeda out of Afghanistan winds down. It is essential that intelligence make the transition to the longer-term fight, and the time to begin that transition is at hand.

The adversary is what some call self-organized terrorism. It grows out of a struggle within the Islamic world between secularism and old traditions. With grassroots origins, the adversary will morph and adapt, regroup, generate new leadership, shift geographic locus, adjust tactics, and evolve into a collection of cells and networks different from the ones we have engaged fairly successfully since September 11. The goal should be to minimize the frequency and scale of future battles against terrorism before their onset rather than merely to enable the intelligence community to support policy and military operations once crises are in full swing—a reactive task it already does well.

In the war ahead, the adaptable nature of the adversary will demand an equally agile U.S. intelligence effort. More resources and better human intelligence will help. But an agile intelligence community will require something else: that the intelligence community at last dispense with the internal barriers that stifle communications and collaboration. Building an agile intelligence capability will require that internal communications improve, that robust and perhaps formal alliances with external centers of expertise be constructed, and that a genuine multidisciplinary analytic effort blossom and achieve a creative flair that is not typical of bureaucratic enterprises.

Metrics will be needed for measuring progress in the effort. They should include measures of improved communication within the intelligence community, structures that connect the intelligence community to the best and the brightest outside the world of intelligence, and indicators of true analytic innovation. Intelligent risk taking and the ability of individual initiative to overcome bureaucratic caution would be central themes in a successful effort.

James W. Harris is senior analyst for Centra Technology and was formerly chief, Strategic Assessments Group, Directorate of Intelligence, Central Intelligence Agency.

U.S. intelligence counterterrorist programs have actually recorded a fair number of operational successes.

Introduction

The House and Senate intelligence oversight committees are set to conduct a rare joint investigation of U.S. intelligence gaps in the September 11 terrorist attacks on New York and Washington. Rep. Porter Goss (R-Fla.), chairman of the House Permanent Select Committee on Intelligence, has stressed that the investigation is not meant to produce “whom shall we hang” recommendations but should instead focus on constructive remedies to intelligence shortfalls. Nevertheless, Sen. Richard Shelby (R-Ala.), vice chairman of the Senate Intelligence Committee, was sharply critical of Director of Central Intelligence George Tenet during recent public testimony, and it is fair to say that Shelby has a lot of company. What will come out of the intelligence review—new initiatives to combat terrorism or finger-pointing? Will the intelligence community be any better prepared to combat terrorism after the joint investigation has been completed and its recommendations made?

Getting beyond Finger-pointing

Tragedies like the terrorist attacks on the World Trade Center and the Pentagon are certain to produce three tribulations: (1) hot-tempered and hastily written allegations of intelligence failure in the popular literature, (2) postmortem studies of the intelligence record by groups inside and outside government, and (3) follow-on official commissions advocating far-reaching reorganization of the U.S. intelligence apparatus. Of those three things, only one—hard-hitting postmortems—is certain to be useful, and several such studies are under way or on the drawing board.

The actions suggested by follow-on official commissions never seem to eliminate subsequent intelligence shortfalls. Finger-pointing has a singularly unproductive history. The mission of the intelligence community has been revisited since the end of the Cold War. Countless reorganizations later, the intelligence community has not yet been “fixed” to the nation’s collective satisfaction. If there is blame to assign, it must be shared by the intelligence community and those who have had a hand in “reforming” it, such as the Church and Pike Committees in the 1970s and other reform efforts since then.[1]

It would be fair to point out that U.S. intelligence counterterrorist programs have actually recorded a fair number of operational successes, as noted in a balanced assessment of what intelligence can and cannot be expected to accomplish.[2] For example, the intelligence community is publicly credited with thwarting planned attacks on the Lincoln and Holland Tunnels in 1993 and attacks against airports on the West Coast on the eve of the millennium.[3] But intelligence cannot achieve omniscience, and if we wait long enough we are bound to be surprised by unfolding events. Osama bin Laden founded the structure that became al-Qaeda during the Afghan war against the Soviets, and it took him two decades to achieve his present notoriety.

What Really Surprised Us about September 11?

It is not as though the intelligence community had never contemplated assaults on the American homeland. In his unclassified testimony of February 7, 2001, Tenet effectively described the sorry state of Afghanistan, the corruption of the Taliban, and the danger posed by the al-Qaeda network:

> Terrorists are also becoming more operationally adept and more technically sophisticated in order to defeat counterterrorism measures. For example, as we have increased security around government and military facilities, terrorists are seeking out “softer” targets that provide opportunities for mass casualties.[4]

He warned plainly of the threat to U.S. citizens from bin Laden, noting that terrorist assaults appeared increasingly likely to be directed against “soft targets” rather than against U.S. military assets, as was the attack on the USS *Cole* in October 2000.

Before September 11, the public was probably lulled by a drop in press coverage of terrorist attacks, the statistics about relatively few casualties from terrorism, and a misunderstanding of the adversary’s changing approach to risk taking. According to “Patterns of Global Terrorism 2000,” compiled by the U.S. Department of State, the number of terrorist incidents worldwide increased in 2000, but only because of a sharp uptick in assaults against pipelines in Colombia.[5] Discounting the incidents in Colombia, the number of U.S. casualties from terrorism showed no upward trend. The attack on the USS *Cole* did not resonate like an attack on the American homeland would a year later. Partly as a result, terrorism moved down on the list of problems to be dealt with by the. Bush administration.[6] The September 11 attacks, ironically, interrupted the last stage of the administration’s own defense review, which was to focus of the need to retool the Department of Defense to deal with longer-term threats.[7]

In such an atmosphere, providing warning is the intelligence officer’s most difficult task. The devil is partly in the details: it is impossible to preempt a threat without knowledge of the specific plot or plots, and it is almost impossible to unearth all of them. Preempting a general threat, as Tenet was attempting to do in his testimony almost seven months before the assaults on New York and Washington, is even harder. Warning is inconvenient when it calls for a change in our basic approach to a national security issue—such as mandating a real commitment to homeland security—and it is especially difficult when it comes in advance of the specific events that will convincingly demonstrate the need for a policy adjustment.

Inside government, bureaucratic politics and internal organizational struggles for resources are forces that define issues and indeed often carry the day in debates in the intelligence community and on policy. Thus, advance warning of details that would discredit the advocates of business as usual is often unwelcome and can go unheeded. All things considered, and acknowledging that there is no excuse, it is hard to imagine the report or intelligence briefing that would have forced the government to conduct national security business as differently before the tragedy of September 11 as it has in the aftermath.

The intelligence community, and especially the Central Intelligence Agency, has a workforce and information resources that agencies in the rest of the federal government properly envy. Whatever its record before September 11, the intelligence community reacted quickly and constructively to the event. Instead of finger-pointing, therefore, we need to ask in the aftermath of September 11 how intelligence can be brought to the level of efficiency needed in the long term. The likelihood is that terrorist threats against the United States will be here for a generation or more, and what is different and novel about the challenge at hand should be considered. That challenge is considerable.

It is impossible to preempt a threat without knowledge of the specific plot or plots, and it is almost impossible to unearth all of them.

The Challenge of the Long War

What we are seeing is not the more familiar state-supported terrorism, which has been in gradual decline for two decades. Rather, the terrorism we face is decentralized, self-generating, and tied to the existence of failed states and the battle for the soul of Islam. Two dimensions of the threat should disturb us and influence any initiatives taken to improve intelligence.

First, the United States is caught up in what Michael Doran of Princeton University calls “somebody else’s civil war.”[8] In almost every Sunni Muslim country, he points out, there are calls by conservative religious elements for the revival of very old traditions. Those elements view modern Western civilization as threatening the survival of traditional Islam as Western civilization bolsters the real

Table 1
Self-Organized Terrorism Compared with Conventional Military Threats

Dimension	Conventional Military Threat	Self-Organized Terrorism
Organization	Hierarchical, formal	Flat, informal, networked
Leadership	Concentrated, institutional authority	Primarily symbolic, with role in fundraising
Loyalty	A state and a polity	A tradition
Coalition partners	Formal, perhaps shifting	Informal, but likely enduring from conflict to conflict
Command and control	Centralized, with clear power relationships	Decentralized, with no one fully in charge
Role of intelligence gathering and analysis	Powerful, primarily offensive	Weak, primarily defensive
Denial and deception	Useful, but of secondary importance	Well developed, critical to mission
Doctrinal development	Derived from formal study, historic experience, simulation, gaming	Evolutionary, trial and error
Other security obligations	Numerous, including regional security, peacekeeping, formal alliances	None
Weapons arsenal	Built through formal acquisition; takes years, even decades; resources abundant	Adaptable, evolves quickly via natural selection; resources a constraint
Financing mechanism	Formal budget, funded by taxes	Contributions from nongovernmental organizations, crime, narcotics

We need to ask in the aftermath of September 11 how intelligence can be brought to the level of efficiency needed in the long term.

enemy—secularism. The struggle is not new, but the identification of America as an ally of the enemies of Islam has gathered momentum with U.S. policy support for secular, corrupt regimes throughout the Middle East and with escalating Palestinian-Israeli tensions.

Civil wars are agony for all participants. Economic historian Brad DeLong is one of several authors who recently compared the contemporary struggles among Islamic factions with the Protestant Reformation of the 16th century. He writes: "The parallels are striking: a dominant clergy and aristocracy that seem to have . . . succumbed to materialism; a rising literate middle class; the mass distribution of personal copies of the Holy Book so that people can read it and think for themselves; and then terror—as those who have convinced themselves that they hear the will of God take action. In Europe, it lasted for 120 years—with one-third of Germany dying in the 30 Years War."[9] One can argue the details of those parallels, but is it reasonable to expect that the struggle between secularism and

Muslim tradition will last for another generation or more, and that the numbers of casualties that will result from the struggle will shock American sensibilities.

Second, while the threat from al-Qaeda is different from that from state-sponsored terrorism—because of its grassroots flavor—al-Qaeda differs from many other grassroots terrorist movements, such as Hamas. Al-Qaeda's objectives are on a grand scale rather than local and specialized. Hamas is concerned with the plight of the Palestinians. In contrast, al-Qaeda is quite literally the irregular force that represents one side in the "Islamic Reformation."[10] Thus, it presents an even more radical departure from the models of conventional warfare to which America has been long accustomed—and with which the U.S. intelligence community was originally built to cope. The United States is comfortable fighting adversaries that are similar to itself and is equally comfortable collecting intelligence against such adversaries. But as Table 1 makes clear, the new adversary has a completely different nature, and "mirror imaging" is thus likely to fail. This adversary is an evolving, adapting force—a network with roots that spread everywhere and for which models of deterrence fail.[11]

The protracted struggle will be daunting, and defeating a broad-based self-organized network like al-Qaeda is an unprecedented chore.[12] Vietnam gave us a glimpse of the challenge, but even there the other side featured a government and command-and-control machinery for U.S. forces to target. The al-Qaeda brand of terrorism more closely resembles a virus that morphs as its environment changes. To further complicate matters, individual nodes are capable of evolving their own strategy and "gaming" their opposition, as September 11 so convincingly demonstrated. They are capable of self-healing, dispersal, reassembly, and innovation. Our challenge is to outwit and then outfight an adversary that adapts rather than plans and that remains capable of decentralized changes in strategy against our vulnerabilities.

To gain an appreciation of what may be in store for the United States, it is useful to compare the present stage of terrorism to the days of evolving communism in the 1920s and 1930s. The useful historical metaphor is not an ossified Soviet Union but the early days of largely autonomous, independently operated and financed cells. Those cells organized local labor movements, fostered radical political causes, acted with global reach, and attracted the sympathies of otherwise moderate citizens. What might a U.S. intelligence community—had one existed in anything like its present form—have done to improve American prospects in the future Cold War with the Soviet Union, and what might the present intelligence community do now to protect our interests during the Islamic Reformation?

In many respects we have been lucky that the evolution of the adversary is not more advanced. It seems unlikely, given the course of the war in Afghanistan, that the adversary had a complete prepackaged war plan that could have unfolded autonomously once the battle was under way and that would have been invulnerable to allied strikes against its command-and-control infrastructure in Afghanistan. This is likely to be one of the lessons the adaptable adversary takes from the current war: its combat operations have to be completely scripted well in advance of the first battle so that the larger war cannot be interrupted by unfriendly bombing or ground force operations. The intelligence community needs to ask what further adaptation of the adversary the war in Afghanistan will foster.

The White House and senior intelligence community management should recognize that they have been lucky that the development of a radiological bomb or nuclear device by this adversary is not further along. They have to wonder how long their luck will hold. Has the U.S. intelligence community yet imagined the full range of models of weapons development that the adversary may employ? Is it sensitive to the right signals of the alternative development paths as they may appear in raw intelligence reporting over the next several years? Does this analytic challenge—and others that demand similarly unconventional imagi-

The al-Qaeda brand of terrorism resembles a virus that morphs as its environment changes.

nation—reside only on the drawing board of the intelligence community, and if so why?

The Need for New Approaches to Intelligence

The magnitude of the threat and the fact that the new terrorist groups bear little resemblance to either conventional armies or state-sponsored terrorist organizations ensure that al-Qaeda and its follow-on movements will demand innovations in U.S. intelligence. Changes in the intelligence craft must go beyond redrawing the intelligence organizational chart and redesigning its chain of command. The collection of raw intelligence will remain critical, but it will also remain insufficient against an adversary that is a dynamic, evolving force. No central authority within the network of terrorist organizations can control, or has the responsibility for designing, future operations against our interests. Thus, there is no triumph of intelligence collection that can completely remedy all of our intelligence shortfalls. The intelligence community will win small battles against terrorism, but it is still at risk of losing far larger ones.

Changes in the intelligence craft must go beyond redrawing the intelligence organizational chart and redesigning its chain of command.

In addition to gathering even more raw intelligence, we need to counter the adaptable adversary with our own adaptation.[13] A $30 billion U.S. intelligence empire, coupled with a DoD that vastly outspends even its most threatening rivals, has most of the advantages, to be sure. But hierarchies are handicapped when confronted by flexible, highly adaptable, and networked enemies. A partial list of remedies to U.S. intelligence's shortcomings is given in Table 2. It is not surprising that several of these remedies are either on the drawing board or actually being implemented within the intelligence community. How vigorously they will be undertaken or how quickly they will mature cannot yet be known.

Breaking Down Barriers

The U.S. intelligence community remains handicapped by internal barriers and walls meant to protect intelligence sources and methods—at a time the outside world, by interesting contrast, apparently sees the value in making unprecedented investments in getting connected ("connectivity").

There is no clearer manifestation of stifling hierarchy than intelligence community "stovepipes" that have persisted for years and prevent many of the people working against terrorist targets from effectively communicating with each other. At times, the stovepipes even prevent organizations from becoming aware of each other's existence.[14] U.S. intelligence components working against terrorist targets need the ability to share data and analyses spontaneously (as academic experts do when communicating routinely over the Internet); they should not be forced to deal with a maze of bureaucratic and security-derived obstacles. That is one of the hurdles implicitly referenced by Tenet in the September 16, 2001, admonition to the intelligence community to erase bureaucratic blockages to fighting the war on terrorism effectively.[15] The intelligence community's electronic connectivity in addressing the non-state-sponsored terrorist threat is ironically held hostage to counterintelligence concerns that emanate from threats from state actors—who, unlike al-Qaeda, have ample budgets to staff their own intelligence apparatus and target it against Washington.

It is no coincidence that most multidisciplinary intelligence analysts and collectors function in largely separate electronic compartments.[16] The "need to know" principle, of course, cannot be jettisoned entirely, but the tradeoff between protecting security and promoting collegiality certainly bears recalibration. The current stovepipe approach—which erects barriers to lateral collaboration by restricting communications and rewarding only bureaucratic loyalty within the organization—makes it possible for unrelated intelligence components in different institutions to do essentially the same work against terrorist targets—wasting resources and preventing many professionals from leveraging the efforts of counterparts who remain outside their immediate circle. Good academics

Table 2
Sample Measures to Bolster Counterterrorism

Proposal	Details
Community information technology (IT) architecture	Create seamless IT system that is shared globally; agency systems are mutually compatible and integrated, though heterogeneous and classified
Universal connectivity	All professionals working terrorism are on the same system and can reach one another easily
Full reach network	Identical e-mail, browsing, collaboration suites for all users
Local autonomy	Local users can create a web presence at their volition on the intelligence community classified Internet, enabling more effective collaboration
Spontaneous organization	Communities of interest can assemble as they deem necessary; individual judgments about the utility of organizing carry the day
External research center	Off-campus facility to promote research collaboration and host visitors from academia and the private sector
Counterterrorism “skunk works”	Institution that promotes innovative ideas and creative approaches unencumbered by traditional bureaucratic restraints
Terrorism red teams	Standing groups of experts with the task of simulating the planning of the adversary’s exploitation of U.S. vulnerabilities
Counterstrategy organization	Internal think tank empowered to integrate research, red team, and game results with raw intelligence to develop clear picture of adversary strategy
Denial and deception cell	Special study group charged with countering adversary measures to deceive U.S. and allied intelligence and devising novel means of deceiving the adversary.
Gaming and simulation center	On-campus facility on scale of national war colleges that is charged with gaming terrorism with participation of U.S. and allied intelligence and policy communities
Software development initiative	Program to seed development of software tools to further highly advanced analysis and data processing
Long-term input into development of collection systems	Integrated effort empowered to represent counter-terrorist community in developing long-term collection platforms

invest considerable energy in finding out about the research efforts of their colleagues in other institutions; intelligence community professionals would reap dividends from similar efforts that at least match those of their academic counterparts.

Also, the people fighting terrorism need to break down barriers to their ability to form alliances with external centers of expertise. In recent years the intelligence community has improved analysts' access to all of the resources made available by the information revolution. It is safe to say that intelligence community data systems are unparalleled. Some elements of the analytic community have created outreach programs to get beyond the walls protecting classified data. But for those in the counterterrorism community, more needs to be done to create connections with substantive experts who do not yet have all the security clearances. No organization, not even one large and deep, can have a monopoly on expertise—especially on a subject as complex as the Islamic Reformation.

Creative alliances with think tanks, academics, and other centers of expertise should be a force multiplier. Intelligence community business practices should promote rather than impede informal and mutually beneficial contact between the analyst and the business community. With the stakes as high as they are, some of those prospective relationships even deserve to be formal, institutionalized partnerships.

There is no triumph of intelligence collection that can completely remedy all of our intelligence shortfalls.

Bolstering In-House Analysis

U.S. intelligence must integrate operational intelligence (intelligence that supports operational planning and covert action), at which the community already excels, with true multidisciplinary expertise, thus capitalizing on expertise in politics, demographics, economics, and culture. The original focus of the Counterterrorist Center, created by then–director of central intelligence William Casey, was almost exclusively operational, leaving all multidisciplinary analysis to the Office of Near East, South Asian, and African Analysis and similar components in the Directorate of Intelligence. As al-Qaeda gathered momentum in the 1990s and the Middle East peace process eroded, the burden on operators and analysts alike to put out daily fires intensified, leaving little time for the sort of research and honest digging that was routine in the intelligence community during the Cold War. The press of daily tasks also reinforced the intelligence community's tendency to insulate.

The intelligence community needs and deserves an unparalleled center of excellence on the roots and substance of terrorism—one that makes the time to do its own research while routinely exchanging insights with a well-developed network of allies on the outside. At the very least, the intelligence community needs an analytic effort that carries great prestige rather than one subordinated to supporting operational planning and covert action.

In the course of bolstering analysis, there is considerable room for more creative approaches, and it makes sense to ask if the intelligence community needs its own analytic "skunk works" to foster such methods. These approaches include assembling "red teams" whose purpose is to simulate adversary strategy and doctrine, perhaps replicating, to the extent feasible, the decentralized nature of the threat. Military intelligence units do this from time to time during conflict, and the DoD has become adept at using this approach to test its own vulnerabilities. The intelligence community should be equally practiced at exploring adversary strategy, especially that of an evolving, adapting enemy whose future stratagems are not yet on the drawing board. The analysis of adversary strategy should have an identifiable and respected bureaucratic base of operation, informed by the most creative thinking of experts in the defense community and in the private sector. Red team mechanisms should be standing requirements, rather than the one-time experiments that are routinely applied to issues such as terrorist innovation with nuclear technologies.

Table 2 summarizes a series of steps to bolster intelligence that are clearly attainable. They include measures that would enable intelligence community analysts to take advantage of all of the benefits of large-scale information networks that are enjoyed by the academic and research communities that use the Internet: the ability to share data and locate expertise spontaneously and the ability to organize communities of interest as soon as the benefits are evident. Other measures are targeted at institutionalizing alliances between experts in and outside the intelligence community and at fostering creative analytic approaches. Still other steps are meant to sharpen the collection of raw intelligence by taking advantage of deeper analytic expertise, thus better focusing human-source intelligence, signals, imagery, and other intelligence collection systems.

Modeling and Simulation

The intelligence community should develop new software tools to support both data processing and analysis. The intelligence community should be using new techniques to explore the evolution of terrorist networks and their adaptability. One new approach, agent-based modeling, focuses on bottom-up computer simulation of human interaction and generates exactly the form of decentralized, spontaneous organization of social networks that we observe in the formation of political movements and in the world of terrorism. A decade ago, an adaptable network of adversaries could have been spoken of only metaphorically. As agent-based modeling shows, with recent advances in computing power and software, synthetic adversary networks can be built in digital space and their evolution simulated harmlessly. In addition, the intelligence community should routinely adopt the best practices of DoD and the private sector for modeling and simulation. At the same time, the intelligence community should prod DoD to create new warfare models that go beyond evaluating conventional weapons systems. To be able to influence and shape DoD modeling, the intelligence community must become so good at modeling and simulation that it can influence the development of those arts outside its own walls.

The art of analytic gaming remains a uniquely effective tool for assessing the interplay of competing strategies, as senior military officers learn in staff colleges. A properly framed game can shed light on the calculations of both adversaries and coalition partners. It is surprising that intelligence community components have not more robustly and routinely exploited this technique for assessing terrorism. There is now expertise to draw from within the intelligence community and a greater appetite for experimentation than existed a year or two ago.

Those techniques might illuminate many examples of adversary strategy that could surprise us next time. Their strategy may depend on how much the terrorists have learned from the strikes against the United States and the war in Afghanistan. For example, attempts by al-Qaeda to inspire jihad in places like Pakistan failed dismally, but the attacks on September 11 appear to have prompted an unlikely spontaneous partnership with whoever conducted the anthrax attacks in the United States in the weeks that followed. Will the terrorists design their own approach with a more creative view of spontaneous partnerships next time? How does the intelligence community assess their capacity for learning?

The intelligence community should continue to counter denial and deception efforts by terrorist networks. Denial and deception analysis is a relatively new element in the intelligence tool kit and refers to measures to counteract the efforts of U.S. adversaries to escape detection by U.S. intelligence satellites and other collection means, as well as measures to counteract adversary efforts to purposefully mislead U.S. intelligence by generating data that point in the wrong direction. Washington cannot allow the adversary to play games with the U.S. intelligence community by placing false leads and producing false warnings. It is uncertain whether the general alerts issued by the Office of Homeland Security during late 2001 were prompted by clever manipulation on the part of terrorist networks that, if they were paying attention, surely noticed that they had the capacity to take the American economy partially offline for days at a time by allowing their own communications to leak. It may

U.S. intelligence must integrate operational intelligence, at which the community already excels, with true multidisciplinary expertise, thus capitalizing on expertise in politics, demographics, economics, and culture.

be no coincidence that senior al-Qaeda leaders in late 2001 publicly framed future assaults on America as attacks on the U.S. economy. The intelligence community must determine the magnitude of the threat to the economy and the strategies likely to be used in an attack aimed solely at economic destruction.

The realization, on the part of senior management of the intelligence community, of the need for creative new approaches is encouraging. Until shortly after September 11, the intelligence community was not in the traditional multidisciplinary analysis business, but the creation of the Office of Terrorism Analysis within the CIA's Counterterrorism Center changed that. This kind of initiative in analytic methodology holds promise, and efforts to reinvigorate the long-term effort to generate more creative raw intelligence collection are in the works. Moreover, in the last three or four years the Directorate of Intelligence has taken measures to create and sustain "out-of-the-box" analytic approaches to difficult intelligence issues, as well as to develop mechanisms to tap expertise outside the intelligence community. What is needed now is a period of growth and development of those programs and the spread of best practices into the counterterrorism community.

Improving the analytic component of counterterrorism may be the most promising way to ensure that collection initiatives are well focused.

The Focus on What Is Secret

It is de rigueur for an analysis of intelligence priorities to cite the need to invest in human intelligence collection. Indeed, in a speech to CIA employees in May 1998, Tenet cited counterterrorism as an essential reason to strengthen the Directorate of Operations.[17]

The war on terrorism will place intense pressure on all intelligence collection systems, and it may do so for a generation or more. The intelligence community will be tempted to "solve" the intelligence problem by throwing resources at collection systems. Although more resources would help, even with more data the intelligence community is likely to be frustrated by its failure to prevent every attack on U.S. interests. The adaptable adversaries who will make up the future terrorist threat will have the incentives and the means to "game" Western intelligence collection systems. Collection needs to be sharp and focused on what counts rather than hopelessly broad. Ironically, improving the analytic component of counterterrorism may be the most promising way to ensure that collection initiatives are well focused. The issue is not exclusively tactical intelligence but also enabling the counterterrorism community to tailor long-term development of collection systems to targets.

Accordingly, we should dispense with the destructive idea that the analytic corps of the intelligence community should confine its attention to the dimensions of the terrorism problem that play to its "comparative advantage" of secret information. Intelligence community analysts will either have the expertise required to get the job done or not. In the long run, it is the job of the intelligence community to develop both analytic expertise and classified data sources on issues of interest to the national security community. That is, the intelligence community must give priority to collecting the information that the policymakers most need and want.

Metrics: How Will We Know We're Headed in the Right Direction?

If a metric were invented to measure the progress of the intelligence community in the fight against terrorism, there would be tension between the wish to base measurements on results and the desire to base measurements on actions taken by U.S. intelligence agencies. Both metrics are important. The United States must resist the temptation to interpret certain tactical victories, especially those enabled by a convenient but perhaps unique ally like the Northern Alliance, as evidence that it has solved the problem. An adversary intent on surprising us will be comfortable with long lulls in its fight against the United States. Those lulls will not necessarily mean that the United States has won the battle, any more than they did in 1998 and 1999.

If all goes well, some intelligence community initiatives will succeed and other will fail. The successes will be informed by lessons from the failures, which will be short-lived and corrected. Any metric the intelligence community employs to gauge progress—and it must use metrics—needs to make room for intelligent risk taking. According to economist Hal Varian, an American expert in technology and innovation at the University of California, Berkeley, the keys to any successful business community revolution are experimentation, capitalization, management, competition, and consolidation.[18] Applying that paradigm to the U.S. intelligence community, it makes sense to credit the mid-1980s creation of the Counterterrorist Center as the critical first innovation in the fight against terrorism. It was an improvement, but one that did not go far enough. Its mission was almost solely intended to augment the collection of human-source intelligence—not to deepen expertise and produce breakthroughs in intellectual capital that might enable us to outwit the adversary. In those instances in which the terrorists made mistakes, intelligence analysis assisted some successful efforts to interdict terrorist plots against U.S. interests. But intelligence analysis and human-source collection left us vulnerable to terrorist plots in which the terrorists used better tradecraft.

The intelligence community thus needs a more risk-taking and failure-tolerant management approach. This national security issue is not one on which to save pennies or to let the possibility of failure suppress innovative approaches. In the medium term, three broad metrics should suggest progress: (1) connectivity is well established, (2) multidisciplinary analysis is diverse and prospering, and (3) individual initiative reigns supreme. Broader dividends will follow if high scores are achieved on those metrics.

The intelligence community needs a more risk-taking and failure-tolerant management approach.

Progress Improving Connectivity

Other improvements are essential as we complete the innovation phase. For one, the successful intelligence enterprise, like its adversary, will be networked and agile. One indicator is the development of strong ties between intelligence community entities working on counterterrorism issues. That will require creation of collaborative mechanisms that do not yet exist. In particular, professionals in the counterterrorist community who work in different buildings, different cities, and different agencies and on different local computer networks will have the ability to create their own collaborative ties rather than wait for senior managers to authorize them and make the required hardware available. The need to form such ties and use them in countering terrorism will be the final compelling reason to reform the management of intelligence community information systems.

A connected community will be one that knows immediately where to find the specialized bit of expertise or the arcane fact that makes the difference in a piece of analysis or in a clandestine collection program.

One critical step is integrating the Office of Homeland Security into the intelligence community's information networks and its client base for its most sophisticated and elaborate products. The Office of Homeland Security is a new organization with the teething problems invariably associated with a new bureaucracy, but the intelligence community should take on the mission of integrating the office into its operations and analysis.

Strengthening Multidisciplinary Analysis

Multidisciplinary analytic approaches to counterterrorism are new, and they will take time to establish and capitalize intellectually. If all goes well, managers of counterterrorism analysis will make room for research and teamwork under the press of daily deadlines, especially when the current war in Afghanistan wanes and demands for current intelligence support are less pressing. Perhaps the most telling measure of the health of the intelligence analysis function will be how the transition from the current war to the longer-term fight is handled and whether analysts are given the chance to take the time to dig deep and think creatively.

The successful intelligence enterprise can be sufficiently agile if, like the terrorist network, it is driven largely by individual initiative rather than commanded entirely from the top.

If developments are moving along the right track, the more creative approaches to analysis will be well staffed, reasonably funded, and institutionalized within the counterterrorism community. No approach would remain untested for its applicability to the counterterrorism problem. The output would be reports and briefings based on research, workshops, conferences, games, red teams, advanced data processing, advanced analytic software, and collaboration across agencies and institutions—not to mention the improved collection of raw intelligence that all of this may help to make possible. The optimum mix of approaches will take time to determine, but it will be diverse and not focused exclusively on current analysis.

There must also be accountability. Eventually, clever approaches must produce both actionable products and new intellectual capital, which would be shared within the community at large. High standards must apply to the new counterterrorism product line.

Fostering Individual Initiative

Common wisdom is that the U.S. intelligence community is so vast and its organizational structure so complex that changing its leadership or altering its organizational chart is not likely to accomplish much. But lessons drawn from the hierarchical, military model can miss the point. The successful intelligence enterprise can be sufficiently agile if, like its adversary, the terrorist network, it is driven largely by individual initiative rather than commanded entirely from the top. Senior intelligence community leaders, while being careful in crafting their daily message to the Oval Office, need to engage in creative delegation and promote initiative and creative thinking (including so-called out of the box thinking) by the workforce.

Another reason to empower individuals is the efficiency gains produced by reducing layers of supervision. The intelligence community is not only stovepiped, it is riddled with layers of management designed to provide redundancy in an effort to avoid mistakes. Analysts have traditionally been subject to multiple layers of supervisory review, as well as to additional review by editorial staffs. Although there has been an effort to streamline the review process in recent years, there remain abundant economies to be realized by placing the individual analyst closer to the decisionmakers who are the end users of the product and relying on individual accountability to ensure quality.

Emphasis on the individual would represent a sharp break with the past. Intelligence community senior leaders are accustomed to being the authors of new initiatives rather than their enablers. Meanwhile, managers and senior analysts climbing the ranks are used to avoiding risks that would take them off the fast track. The tendency to confine risk taking to the top and to constrain individual initiative because it might lead to a mistake is one of the things that must change if the fight against terrorism is to succeed.

Conclusion

Good intelligence will accomplish only so much. Policymakers must also be inclined to new approaches, and they need to be receptive to messages from the intelligence community that are inconvenient to the daily policy agenda. The intelligence community will be doing its duty if two things that mark all successful intelligence enterprises are mastered: (1) forging a close connection to policy and (2) being persistent when it has to persuade an audience of the need to do something different. The intelligence community must have the will to resist the temptation to sacrifice one of those things for the sake of the other.

Two indicators will be telling. First, the "resource mix" in the intelligence community must be optimized without being held prisoner to debilitating bickering. One vulnerability is likely to be internal intelligence community struggles over resources, as competing collection systems argue the case for more people and funding at the expense of each other and at the expense of creative analysis. By focusing excessively on any one intelligence collection resource, including human-source reporting, we run the risk of producing occasional operational successes (when the intelligence community is fortunate enough to get access to just the right cell or terrorist communications channel) at the expense of preventing national traumas in other instances (when the terrorists are merely lucky or when they outsmart our best efforts). This is a principal legacy of September 11. Strong intelligence community leadership and alert congressional oversight can avert such an outcome.

Second, when all is said and done, the joint House and Senate investigations will need to focus on intelligence community culture and business practices, not merely on the organizational chart. That means going beyond finding scapegoats and redrawing lines of subordination and hierarchy. And the professionals who are in the business of intelligence gathering and analysis must be part of developing the solution, not merely held responsible for implementing a plan designed by an outside group. If those professionals are doing business as usual several years hence, we will have failed to get it right.

In sum, the intelligence community needs to become as agile and as innovative as its terrorist adversary. It can take constructive cues from counterparts outside the realm of intelligence collection or analysis: the network of experts and data sources in the nation's best think tanks, its best universities, its best war colleges, its best consultancies. It is a matter of where to set the bar and how to unleash the intelligence community's talents. Better communications, an emphasis on individual initiative, reducing bureaucratic barriers, and boosting multidisciplinary analysis are keys in the months ahead.

Notes

[1] The Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Sen. Frank Church (D-Idaho), was established on January 27, 1975, to investigate abuses by intelligence agencies. The committee focused on major reforms. Parallel investigations were conducted by another committee chaired by Rep. Otis Pike (D-N.Y.).

[2] Richard K. Betts, "Fixing Intelligence," *Foreign Affairs* 81, no. 1 (January–February 2002).

[3] Ibid.

[4] www.cia.gov/terrorism/index.html.

[5] U.S. Department of State, www.state.gov/s/ct/rls/pgtrpt/2000.

[6] Barton Gellman, "A Strategy's Curious Evolution," *Washington Post,* January 20, 2002.

[7] Portions of the defense review did concern asymmetric and other forms of "Fourth Generation Warfare." An early introduction to these issues can be found in Martin Van Creveld, *The Transformation of War* (New York: Free Press, 1991).

[8] Michael Doran, "Somebody Else's Civil War," *Foreign Affairs* 81, no. 1 (January–February 2002).

[9] Brad DeLong, www.j-bradford-delong.net/TotW/Islamic_Reformation.html.

[10] Stressing the global nature of the threat, Tenet is reported to have told the cabinet principals in the days immediately following September 11, "You've got a 60-country problem." Dan Balz, Bob Woodward, and Jeff Himmelman, "Ten Days in September," *Washington Post,* January 27, 2002.

[11] This discussion draws from two streams of literature, one dealing with self-organization and the other with network-centric warfare as applied to terrorism. Representative of the first is Stuart Kauffman, *At Home in the Universe: The Search for the Laws of Self-Organization and Complexity* (New York: Oxford University Press, 1996). The second is represented best by David Ronfeldt and John Arquilla, "Networks, Netwars, and the Fight for the Future," on First Monday.org, October 2001, www.firstmonday.org/issues/issue6_10/ronfeldt/index.html. Ronfeldt is a senior social scientist at RAND, and Arquilla is a professor at the Naval Postgraduate School.

[12] Self-organization and the operation of networks are relatively new ideas in the conduct of warfare. Self-organization refers to the propensity of the elements of a system to establish order without central oversight, as though doing so spontaneously. The idea is especially germane to biological and political systems, in which cells begin to work synergistically—in the early development of an organism or when a political move-

ment is quickly "born" of commonly shared but only recently formed opinions. Financial markets also exhibit self-organization when bubbles are created out of the dynamics of expectations of individual participants. Networks also exhibit emerging structure as nodes are added and connectivity multiplies disproportionately. For further information, see Kauffman; and Ronfeldt and Arquilla

13. Experts at the RAND Corporation make similar recommendations for countering adversaries on the conventional military battlefield: the U.S. military counters dispersed, decentralized foes with "swarming tactics" that are enabled by the adaptability of our own forces. See, for example, John Matsumora et al., "The Army after Next: Exploring New Concepts and Technologies for the Light Battle Force," RAND Corporation, DB-258-A, 1999, www.rand.org/publications/electronic/ force.html, and the list of other publicly available publications on the RAND website.

14. The creation of the Counterterrorism Center in the mid-1980s was intended to achieve improved connectivity by bringing together professionals from different intelligence and law enforcement agencies. For its day, the CTC was a dramatic step in the right direction. The CTC, however, was conceived as a largely operational entity and lacked strong ties to the broad community of intelligence analysts and to other centers of multidisciplinary expertise outside the intelligence community.

15. The message has been referenced frequently in the press and in other literature. See Betts.

16. Analysts directly supporting the collection of raw intelligence are not so removed.

17. See www.cia.gov for the text of the speech.

18. Hal Varian, "Five Habits of Very Effective Revolutions," *Forbes ASAP*, February 21, 2000, www.forbes.com/asap/00/0221/073.htm.

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001, call toll free 1-800-767-1241 (noon - 9 p.m. eastern time), fax (202) 842-3490, or visit our website at www.cato.org.