Frank J. Cilluffo, Ronald A. Marks, and George C. Salmoiraghi

The Use and Limits of U.S. Intelligence

After spending nearly $30 billion annually on intelligence gathering efforts, why did the intelligence community (IC) fail to predict the September 11 terrorist attacks? How could they have prevented the attacks? How can the United States improve its ability to ensure that an event like this will not happen again?

The role of U.S. intelligence cannot be minimized; it will be Uncle Sam's lifeblood in the campaign against terrorism. Accurate and timely information is the foundation of every element of this campaign, including U.S. diplomatic, military, financial, and political operations; it also provides warning of future attacks. At present, the IC has not received sufficient funds to accomplish its tasks or sufficient political support when the inevitable failure occurs. Ironically, at the dawn of the information age, the United States has neglected its own intelligence foundation.

What exactly is "intelligence"? Classic espionage is defined as an "intelligence activity directed toward the acquisition of information through clandestine means and proscribed by the laws of the country against which it is committed."[1] Intelligence involves understanding the motivations, thoughts, and plans of one's enemies. Multidisciplinary intelligence, including insights into the cultures and mindsets of terrorist organizations, is crucial to providing indications and warnings of possible attacks and is critical to illuminating key vulnerabilities that can be exploited and leveraged to prevent, preempt, and disrupt terrorist activities before they occur. The first priority should always be to get there before the bomb goes off.

Frank J. Cilluffo recently chaired two committees on homeland defense, including one on combating terrorism, at CSIS. Ronald A. Marks is a former officer at the Central Intelligence Agency and former intelligence counsel to Sen. Bob Dole (R-Kan.) and Senate Minority Leader Trent Lott (R-Miss.). George C. Salmoiraghi is an attorney and research associate with the Global Organized Crime Project at CSIS.

The Washington Quarterly • 25:1 pp. 61–74.

The United States must now build quickly on the centers of excellence in intelligence that already exist and improve the areas in which deficiencies are found. Decisionmakers must provide the IC with the tools it needs to do its job. Energies and resources must focus on ameliorating, not degrading, current conditions and capabilities. If required at a later time, our leaders will certainly hold the responsible parties accountable during the requisite "blame game." (As a cautionary note worth repeating, successes go unheralded while failures make the headlines in the intelligence gathering business.)

Why the United States Slept

Understanding the historic relationship between the United States and the necessarily shadowy world of intelligence is important. U.S. citizens have been of two minds about the subject, vacillating between their fascination with intelligence's romanticized, James Bond–like aspects and their repugnance at its reality, in which "dirty people" engage in "dirty business."

During the Cold War, U.S. efforts to collect intelligence focused on the Soviet Union. After the Soviet Union's collapse in 1991, the transnational hydra supplanted the Russian bear. As James Woolsey, former director of central intelligence (DCI) at the Central Intelligence Agency (CIA), noted, the "dragon" was gone, but "a jungle full of poisonous snakes" had replaced it.[2] Rather than facing a monolithic adversary, the United States was challenged by a worldwide range of threats—from terrorism to organized crime to narcotics trafficking—all difficult targets to pinpoint.

The mid-1990s saw the swing toward the "cleaner" intelligence method of signals intelligence (SIGINT) and away from human intelligence (HUMINT) in a manner unseen since the "rogue elephant" days of the 1970s; budget cuts and reductions-in-force followed. Paralleling the sentiments of President Jimmy Carter and former CIA director Stansfield Turner, senior advisers in the Clinton administration displayed open hostility toward the IC, particularly toward HUMINT.

This focus on "clean" SIGINT has been the hallmark of the past 10 years in intelligence collection. SIGINT continues to prove its enormous value in collecting information about such things as the location of tanks or some telephone conversations, but SIGINT was unable to provide any insight into what a particular cell was planning. That type of information requires a person.

Simultaneously, case officers have been required to make sure that their human assets were clean—free of human rights violations and able to pass a litmus test of positive attributes—or that they were "boy scouts," as one clandestine service officer referred to them. The CIA established these

guidelines in response to the murders of a U.S. innkeeper and another U.S. citizen's Guatemalan husband by a Guatemalan army officer whom the CIA had recruited. Even though the specifics are classified, the guidelines establish a balancing test that weighs the value, or potential value, of the intelligence gathered against the person's record of human rights abuses. Recruitment of such a "dirty" asset would then require approval at the highest levels in CIA headquarters. This "transparency" was designed to protect and embolden officers to recruit others by ensuring concurrence on the part of headquarters. In practice, however, this procedure has deterred officers, instead of encouraging them.

> Accurate and timely information is the foundation of all elements of the campaign.

To obtain the information required to protect the lives of U.S. citizens, dealing with people who have blood on their hands is necessary. The concept that "gentlemen don't read one another's mail," although graced with laudable intentions, is based on the principle that in an ideal world there would be no need to spy on one another. The grim reality is that terrorists are not gentlemen. Sadly, by not recruiting people who lower themselves to the level of terrorists, the IC loses everything.

Finally, defending the IC became politically unpopular when the inevitable failure occurred. Too often, politicians nailed the pelts of scapegoats to the wall in order to appease a skittish public. This cool bureaucratic climate, in turn, affected the risk-benefit calculation that determines not only what information is required and how it is collected but also what is not collected. Obtaining the necessary information without dealing with the dirty guys is impossible.

Sharpening Counterterrorism Tools

Winning Hearts and Removing Masterminds

Part of the campaign against terrorism involves exploring novel and more effective ways to disseminate information. To be maximally effective, the U.S. response to the September 11 attacks should include a robust and integrated campaign of psychological operations (PSYOPS). PSYOPS are used to induce supportive behavior. According to a study that the Defense Science Board released in May 2000, military PSYOPS are

> [p]rograms of product and/or actions that induce or reinforce the attitudes, opinions, and emotions of selected foreign target governments, organizations, groups, and individuals to create a behavior that supports U.S. national policy objectives and the theater combatant commander's intentions at the strategic, operational, and tactical levels. PSYOP events are planned, coordinated, and executed before, during, and after conflicts.[3]

Controlling the "soft" battleground can shorten the length of the conflict and can help determine how the struggle will affect long-term strategic interests.

The United States successfully used PSYOPS during the recent conflicts in Iraq, Somalia, and the Balkans. These tactics continue to provide support to the peacekeepers on the ground in the Balkans and helped establish an environment where democratic elections engendered a comparatively smooth transfer of power.

For the United States to address the cultural environment in which terrorists and their organizations take root is a crucial step in creating a climate in which they are unwelcome. In turn, this outcome can shorten the conflict by eliminating or limiting the terrorists' base of support. In addition to dropping bombs, the United States should continue to air-drop supplies to the Afghan people. Providing relief materials—food or medical supplies wrapped in the U.S. flag—makes a tremendously powerful statement.

The United States must also draw a crystal-clear line and place the radical extremists on the other side of it. This battle is not against religion; it is a counterattack against madmen. The U.S. message, which should explain the repercussions of supporting terrorists, could be used to demoralize the enemy, thereby lessening its will to fight. The campaign would need to erode the terrorists' popular support as well as isolate the military and the operational planners from the larger organization, isolate organizations from each other and from the larger "movement," and ultimately separate the movement from society at large. As long as the terrorists' cause finds a supportive environment, terrorism can take root. In many ways, the most effective means of dealing with terrorism is to "drain the swamp" where these people live. Isolating terrorists from society substantially diminishes their ability to organize and finance their training and operations, as well as to recruit soldiers. PSYOPS are particularly significant in such a context: fighting fire with fire and ideas with ideas is important because that is as close as one can get to "rooting out" the problem.

On this issue too, the United States should reach out to third-party countries, in this case most notably Indonesia. Despite popular misconceptions, the majority of the world's Muslim population lives in Southeast Asia, not in the Middle East. Muslims in Indonesia could provide a valu-

able cache of support for the likes of Osama bin Laden in the world, as well as the basis of an international network that could destabilize the governments of the entire region, thereby drawing the world into further conflicts.

Finally, the United States could control future events by neutralizing misunderstandings and misperceptions about U.S. foreign policy and the country's citizens. The dissemination of these messages is necessary to contribute to a safer world after the United States has responded to the terrorist attacks. In general, terrorism has always been a weapon that the weak use to target the strong. It is a low-cost, high-leverage method that enables small nations, subnational groups, and even individuals to circumvent the conventional projections of national power—political, economic, or conventional military might. Part of the changing face of international terrorism, referring to al Qaeda in particular, involves the terrorists' ultimate objectives. These networks no longer seek a seat at the negotiating table; instead, they want to blow up the table and build a new one in its place. In light of this shift, the United States requires a clearly defined military, political, and economic objective as well as strong international support.

The U.S. response should include a campaign of psychological operations.

Problems arise because neither al Qaeda's suspected mastermind, bin Laden, nor the Taliban is susceptible to traditional international pressures. Their particular brand of radical Islam, one that the Muslim community as a whole finds distasteful, insulates them from established geopolitical machinations. These groups' allegiance to their ideals frees them from confronting some of the pressures that face human beings—these radical fundamentalists answer to no one but their God. To isolate them further from the community of nations is all but useless because their aspirations transcend the concept of the nation-state.

In the long term, bin Laden and his al Qaeda network seek to establish an Islamic world. In the short term, bin Laden has targeted several Middle Eastern nations, most of them with ties to the United States, as having the potential to become radical Islamic states. In addition to spreading his hatred of the United States, bin Laden seeks to undermine these nations' support for the United States; he is also blackmailing these nations to make them more receptive to his ideas. This depiction is not intended to portray him as a superhuman puppet master but rather to demonstrate that his instructions have been issued and his actions justified on religious grounds. Bin Laden's beliefs

are a venomous strain of Islam, a warped version. Perhaps the greatest threat to Islam is bin Laden himself. Indeed, radical Islamic militants—a minority within the overall Islamic community—constitute his base of support.

Isolating the smaller core of "true believers" from the rest by emphasizing the extreme nature of the crime committed against the United States might be possible. To do so, the world must delegitimize terrorism as a viable option by reaching a consensus that terrorism will not be tolerated and by forcing those who engage in terrorist activities to face international retribution.

Exploiting and Attacking Terrorist Infrastructures and Communications

Another effective tactic involves disrupting terrorists' abilities to communicate with one another and with the rest of the world. Terrorists rely on both high-tech and low-tech means of communication. Bin Laden's primary means of communication with his network's members had been the Internet; what role it played in the attack on September 11 remains to be seen.[4] The U.S. IC's ability to observe the Internet passively and trace communications among individuals and cells is crucial to the campaign against terrorism.

Dealing with people who have blood on their hands is necessary.

Al Qaeda presents a particular challenge because it is a network of networks of networks, in which terrorists from various organizations and cells pool their resources and share their expertise. This loose affiliation does not have the clear lines of communication of a centralized command structure, such as that provided by an army general or a corporate chief executive officer. The network is, instead, a "combination of convenience," with groups joining and departing, depending on their interests and the needs of their particular operations.

The terrorists have a communication network similar to the informal, unregulated *hawala* system of passing credited money from one trusted friend to another. Feeding false information into this system would go a long way toward disrupting terrorist groups' daily operations and eventually eroding internal trust. Studying the rise and fall of the Abu Nidal organization, whose downfall can be attributed to the leader's loss of confidence in his people, may have merit. Strangely enough, the vilest terrorist depends on the "honor" of another terrorist to do his or her work. Once that honor or loyalty is viewed as breached, the system of trust—the glue of the organization—collapses.

The Way Forward

The breadth, depth, and uncertainty of the terrorist threat demand significant investment, coordination, and retooling of the intelligence process across the board for the preattack (warning), transattack (preemption), and postattack (investigation) phases.[5] This effort requires strengthening "all-source intelligence" capabilities, meaning both SIGINT and HUMINT, at every phase of the intelligence cycle: collection, processing, analysis, and dissemination. (The intelligence cycle is not linear, but circular: once intelligence is disseminated, new questions arise that require a new round of collection, processing, analysis, and dissemination.)

As a threshold matter, the intelligence services in the United States need to be placed on a wartime footing. Temporary task forces focusing on terrorism are not enough. The larded bureaucracy of the 1990s needs to be reshaped immediately to support homeland defense. This step requires the CIA to recognize the primacy of the Counterterrorism Center and to direct the proper resources, personnel, and funding on a sustained basis to confront the situation in this new world—and not merely just for the duration of the battle. Notably, some time may pass before the intelligence agencies are able to correct the deficiencies that years of tepid political support have entrenched. Many of the solutions relate to the culture of the IC organizations—both within an agency or organization as well as between various agencies and organizations.

To date, SIGINT has provided decisionmakers with the vast bulk of operational information on counterterrorism. National technical mechanisms cannot be allowed to atrophy further. In reality, however, all-source intelligence provides the only viable means of obtaining timely intelligence. Both HUMINT and SIGINT capabilities should be bolstered.

Some of the largest areas of potential improvement lie in utilizing the overlap between the two intelligence disciplines—using SIGINT to reinforce HUMINT, and vice versa—to develop innovative synergies. In addition, the "signal-to-noise ratio" must be improved. Because officials received dozens of threats each week, the agencies must develop mechanisms to separate actionable intelligence from empty warnings.

Collection Capabilities

Like everyone in the world, the U.S. IC has suffered from the dizziness of dealing with too much information in today's information age. As a result of restrictive budgets, the IC continues to use a hodgepodge of aging and incompatible electronic data systems to deal with an ever-expanding stream of data. The community is also engaged in the wholesale rejection of nonclas-

sified sources of information. This concentration on secret or restricted-access sources is laudable in a time of crimped budgets and limited goals. The vast amount of so-called open-source information, however, must be examined in detail as a resource that the new terrorists use for everything from passing "private" messages to recruiting members to promulgating their ideology to the masses. The IC needs more money for a new information infrastructure and a new approach to open-source information.

Even the vilest terrorist depends on the 'honor' of another terrorist.

In the more traditional area of data collection, better imagery and signals intelligence requires more "air breathers" (unmanned aircraft fitted with high-tech surveillance equipment) and fewer "non–air breathers" (space-based satellites, also outfitted with high-tech surveillance equipment). The United States relies on a number of highly sophisticated fixed-orbit satellites. Their orbits have been studied and plotted, and their location at any given time can be calculated. Consequently, the satellites' predictability diminishes their utility, because malfeasants essentially know when the "eye in the sky" will be trained on them—and they act accordingly. Increasing the number of air breathers provides a potential solution to this predictability. Because they do not maintain a fixed and well-understood schedule, adversaries cannot schedule their activities around the unmanned aircraft. Handlers can also focus these aircraft on a specific target or targets for a longer period of time.

Yet neither of these modes of collection offers insight or access into the minds of the terrorists. Therefore, the IC needs HUMINT—people placed within the decisionmaking chain of the terrorist organization with access to the group's plans and intentions.

HUMINT is the weakest choice in the IC's current toolbox. As a result of the bureaucratic and political fears of associating the CIA and the United States with human rights abusers, in 1995 the DCI issued guidelines detailing complex procedures for gaining approval to recruit informants who may have run afoul of human rights laws. In theory, these guidelines were designed to further insulate and protect the CIA. In practice, however, they had a chilling effect on the recruitment of potentially useful informants because they discouraged CIA case officers from recruiting the types of sources needed for effective collection efforts. The procedures established a risk-averse climate and forced the United States to rely on foreign intelligence services.

Decisionmakers should relax or entirely discard the guidelines to allow intelligence officers to recruit not only terrorists but also others with, at

best, questionable human rights records. HUMINT truly is a twilight struggle. The IC must deal with individuals who are unsavory and dangerous. Interaction with them does not imply approbation of their previous actions but recognizes that the potential value of their knowledge—information that can save the lives of U.S. citizens—outweighs the disagreeable background of these sources.

This approach will require a new breed of case officer, because terrorists do not frequent the cocktail party circuit or similar circles. The next generation of field officers will need to be well versed and grounded in the language and culture of the region under investigation. They will need the ability to deal not only with government officials but also with shopkeepers and the like. In the words of Rudyard Kipling, they will need to "walk with Kings—nor lose the common touch."[6]

Naturally, this approach increases counterintelligence concerns. Dealing with less reputable people requires increased vigilance on the part of the IC as a whole. We need to be willing to accept increasing counterintelligence efforts and understand that the United States will occasionally get "stung." Recruiting an asset necessarily involves a cost-benefit analysis. When moving in the realm of smoke and mirrors, sometimes you are left grasping at nothing, and sometimes you bang your shin. Getting stung is sometimes the price of doing business, particularly when the prize is worth it. This recognizable risk should be accepted.

> Once that 'honor' is viewed as breached, the glue of the organization collapses.

These officers will need greater support from their organizations. Oversight by the parent agency of the actions of officers in the field is vital. The line between supervision and micromanagement, however, is thin. For example, paying bribes is an age-old and indispensable part of intelligence gathering, and the officer must be in a position to take advantage of this method. The current authorization process should be streamlined in order to allow the officer greater responsiveness and flexibility in the field, but should still maintain its crucial regulatory role. After all, James Bond never had to fill out paperwork or myriad bureaucratic forms.

Processing the Information

No one has any use for intelligence that is gathered and not processed—that is, teased out for the most relevant and timely pieces of information. Several times in the past few years, the IC has had information about an event but, at least for a while, had no knowledge about the data's location.

In an age of split-second timing and attack, the IC must be equipped with proper, modern computer systems—which the private corporate sector has had for years—to mine the flow of data received from satellites, the Internet, and dozens of other sources. This solution does not involve sexy spending, but it is a vital step, which also needs to be better organized within the IC and its programs, each of which has its own plan for technology acquisition.

Additionally, the IC has not sufficiently invested in so-called fusion analysis. This examination, in which computer systems and software are used to extract and compare multiple sources of information and databases, would prove extremely valuable in the byzantine world of terrorism roots and root systems tracing, including in such areas as finances, personal connections, and so forth. Fusion analysis could also be used to develop the sorely needed deep databases that the IC often lacks. The IC, like other government bodies, faces fading institutional memories and all too often is forced to rely on incomplete paper records.

Analysis

At its best, analysis involves converting basic raw information into finished intelligence. Aside from being steeped in the language and culture of the area or region in question, analysts need to integrate various streams of data into a coherent whole. In the wake of the cutbacks of the 1990s, the IC faces a dearth of people with the necessary linguistic and cultural skills to accomplish this task. The remaining skilled individuals have been organized into an increasingly bureaucratic system that is top-heavy with layers of management and fundamentally out of touch with the policymakers they are supposed to serve. The various agencies that make up the IC—the CIA, the Defense Intelligence Agency, and others—need to attract people with the necessary language and cultural skills now, pay them well, and find ways to retain them. In addition, agencies must simplify the strangling overhead that separates the analysis from the customer.

Dissemination

Once the intelligence is fully collected, processed, and analyzed, the information needs to find its way expeditiously into the hands of decisionmakers and others—such as law enforcement agencies and the military—who can act on it. Unfortunately, these parties do not always get what they need when the need it; nor do they always get it in a useful format.

The limitations placed on providing intelligence to law enforcement must continue to be adjusted. Information that is not received or that is too

highly classified is worthless. The need to protect various sources and methods requires a classification system. Too often, law enforcement personnel who could make the most use of timely intelligence do not have access to it. The means do exist whereby knowledge can be shared without needlessly endangering sources or methods; these systems must be refined to work more efficiently. This situation is part and parcel of the historical lack of cooperation between the intelligence and law enforcement communities.

Despite improvements in past years, agencies involved in intelligence and law enforcement do not always share the same goals. Law enforcement wants to string criminals up, whereas the IC wants to string them along. Intelligence agencies have been reticent to share information with law enforcement because of the desire to prevent discussion about their sources and methods in open court, a situation that would reveal this information to the world. For their part, law enforcement agencies in the United States must move beyond the usual case-busting aspects of their normal work and provide intelligence analysts with the information they receive from their sources.

Both human and signals intelligence capabilities need to be bolstered.

The past few years have produced substantial improvements in cooperation between the two communities. This outcome is partly a result of assigning, or exchanging, individuals temporarily from one community to the other, also known as detailing. For example, the communities have come together on their joint counterterrorism mission. The IC's Counterterrorism Center is staffed with members from the various agencies that have antiterrorism and counterterrorism responsibilities. These improvements will likely continue through the efforts of the newly created Office of Homeland Security, headed by former Pennsylvania governor Tom Ridge.

Furthermore, promoting the exchange and propagation of information among and between all parties with responsibilities for antiterrorism and counterterrorism efforts is important; the information flow must involve the highest levels of the federal government as well as state and local governments. The methods and technology that allow classified information to be shared with individuals who do not have clearance also need to be strengthened without endangering sources and methods. In addition, officials must develop a method whereby information flows up from local levels to the federal level.

Similarly, in this sort of campaign, intelligence and military officers will both play essential roles in coordinating U.S. actions. Therefore, both must strengthen and improve mutual channels of communication. The current gap hampers smooth interagency and interservice activities.

Moreover, understanding motivations and discovering potential actions are as important to the current campaign as dropping bombs on, or directing troops to, a particular target. The IC must better understand its military customers and their different levels and types of need. For example, to carry out assigned duties, the commander in chief of the U.S. Central Command, who focuses on the Middle East, needs information that has a broader focus and is more policy oriented than does the captain of a Special Operations Command that is reconnoitering on a terrorist base in Afghanistan.

Finally, government officials cannot allow international borders to stop the flow of information in this campaign, where seamlessness is key and success demands cooperation with foreign governments. In many situations, foreign allies have access to information that the United States lacks and does not have the time to develop. Moreover, the United States should not have to reinvent the wheel; U.S. decisionmakers could learn from those nations that have had substantial and prolonged experience dealing with terrorists and terrorism. The United States could draw from the lessons that these countries learned and structure policies accordingly.

The Limitations of Intelligence

The IC's capabilities and efforts alone, no matter how robust, will never be sufficient. The United States cannot prevent all attacks all the time. Good leadership involves accepting responsibility for successes as well as failures.

Rebuilding a strong intelligence capability takes time and sustained effort. Many have called for an increase in the number of officers assigned to clandestine activities. Without question, this step is necessary. Time and money, however, is needed to train new officers. Patience is therefore required. After all, airborne troops do not sign up one day and jump out of an airplane the next. Individuals with close familial and cultural ties populate the closed world of terrorism. Penetrating their networks takes time—often more time than other areas of espionage require. In many cases, penetrating these organizations will be impossible, but recruiting members of a group's decisionmaking chain may be possible. Even with people on the inside, however, exact predictions are simply not possible.

Analysts are estimators, not clairvoyants. In the best of circumstances, a well-trained analyst cannot read an opponent's mind. Analysts can explain a trend or understand a motive, but they will not know everything. Policymakers will need to accept the limitations of intelligence efforts. In the nether world of compartmentalized cells—each consisting of three or four people—intelligence gathered will be circumstantial, not conclusive.

In general, spies collect information; law enforcement agents collect evidence. This cultural difference affects the use and effectiveness of information. The system is not going to change, and society does not want it to change. The gaps separating the two communities cannot be closed entirely, but they can, and must, be bridged.

Additionally, expanding the conceptions of the strengths and limitations of various agencies that have not historically been part of the core activities of the IC is important. In particular, the Department of State plays a crucial role in diplomatic relations as well as in efforts to limit various countries' abilities to act as illicit tax havens. Similarly, the Department of the Treasury has targeted various malfeasants' financial assets to weaken these opponents economically. These necessary elements of the campaign require a different sort of intelligence and a different sort of officer. Recognizing that traditional notions of intelligence may need to be expanded to accommodate new tactics and requirements is important.

Analysts are estimators, not clairvoyants.

Many have suggested the desirability of increasing covert action against nonstate terrorist groups, including lifting the ban on assassinations. Despite media hype to the contrary, assassination is truly difficult, as intelligence officers are well aware. It is dangerous, hand-to-hand warfare with unexpected and limited results. U.S. policymakers must accept these ambiguities—moral and otherwise. Starting and suddenly stopping these types of activities would do little good.

Many of these recommendations call for loosening restrictions, but they beg the question of the role of oversight. Oversight ensures that the actions that intelligence agencies take on behalf of the United States do not subvert the pillars of democracy in an attempt to protect it. A strong intelligence organization is not inconsistent with U.S. values or civil liberties. The Constitution provides room for both. Implementation of some measures, however, requires political fortitude. Responsibility requires taking the good with the bad. Intelligence is neither an infallible nor a benign business. Policymakers and politicians need to accept these facts and occasionally make decisions that are politically unpopular.

Strengthening the U.S. IC is important not only in the battle against terrorism but also for as yet unspecified future conflicts. The IC must be provided with the flexibility it needs to deal with today's problems and to address tomorrow's situations—without requiring such a graphic reminder as September 11. The IC needs to be able to adapt and overhaul itself both in response to, and in anticipation of, future moving threats facing the

United States. The country is capable of successfully prosecuting its current campaign against terrorism, but that success depends on a robust intelligence capability.

Notes

1. Frank J. Cilluffo, remarks to the 1998 World Economic Forum annual meeting.
2. R. James Woolsey, testimony before House Committee on National Security, February 12, 1998.
3. Defense Science Board Task Force, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "The Creation and Dissemination of All Forms of Information in Support of Psychological Operations (PSYOP) in Time of Military Conflict," May 2000, p. 7.
4. See Jack Kelley, "Terror Groups Hide behind Web Encryption," *USA Today*, June 19, 2001; Dan Verton, "Terrorists Use High-Tech Tools, Low-Tech Tactics," *Computerworld*, September 12, 2001; Daniel Seiberg, "Bin Laden Exploits Technology to Suit His Needs," *CNN.com*, located at www.cnn.com; accessed September 21, 2001; Jerry Seper, "Terrorists May Have Used Internet to Plot," *Washington Times*, October 6, 2001; Doug Bedell, "Possible Terrorist Use of Internet Encryption Debated," *Dallas Morning News*, October 12, 2001.
5. See Frank J. Cilluffo et al., *Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy* (May 2001), p. XI.
6. Rudyard Kipling, "If," in *Rewards and Fairies* (1910).