Richard K. Betts

THE NEXT INTELLIGENCE FAILURE: THE LIMITS OF PREVENTION

[Note: This is the original manuscript for an article that appeared in practicallyt the same form as "Intelligence Test," in James F. Hoge, Jr. and Gideon Rose, eds., *How Did This Happen? Terrorism and the New War* (New York: PublicAffairs, 2001) and "Fixing Intelligence," *Foreign Affairs* vol. 81, no. 1 (January/February 2002. Richard K. Betts is Director of the Institute of War and Peace Studies at Columbia University and was member of the National Commission on Terrorism. He is author of *Surprise Attack* (Washington, D.C.: Brookings Institution, 1982) and numerous articles on intelligence.]

As the dust from the Twin Towers was still settling, the chants began: CIA was asleep at the switch! The intelligence system is broken! Reorganize top to bottom! The biggest intelligence system in the world, spending upwards of $30 billion a year, could not prevent a group of fanatics from bringing off the stunning assaults. The new conventional wisdom was typified by Tim Weiner in the *New York Times*: "What will the nation's intelligence services have to change to fight this war? The short answer is: almost everything."[1] Drastic change must be overdue.

Yes and no. A lot must, can, and will be done to shore up intelligence. Reforms that should have been made long ago will now go through. New ideas will get more attention and good ones will be adopted more readily than in normal times. There is no shortage of proposals and initiatives to shake the system up. There is, however, a shortage of perspective on the limitations of improved performance that we can expect. Some of what is done will replace old problems with new ones. The only thing worse than business as usual would be naive assumptions about what reform will accomplish.

Paradoxically, the news is worse than the angriest critics think, because the intelligence community has worked better than they think. Contrary to the image left by September 11, the cooperating network of U.S. intelligence and associated services has generally done very well. Great successes in thwarting previous terrorist attacks are too easily forgotten in the shock of one catastrophe. For example: plots to bomb the Lincoln and Holland tunnels in 1993, to bring down eleven American airliners in Asia in 1995, to mount attacks around the millennium in Jordan and on the U.S. west coast. and to strike U.S. forces in the Middle East in [summer month?] 2001.

The awful truth is that the best of intelligence systems will have big failures. The terrorists that intelligence must uncover and track are not inert objects, but live, conniving strategists. They too fail frequently, and are caught in time, but they will not always fail to find ways to work around a proficient

---

[1] Tim Weiner, "To Fight in the Shadows, Get Better Eyes," New York Times, October 7, 2001, Week in Review, p. 1.

intelligence system. Counter-terrorism is a competitive game. Even minor league pitchers can sometimes strike out a major leaguer who bats .350. When a strike-out means that people die, a .350 average -- or for that matter .900 -- looks far worse than in baseball.

It will be some time before the real inside story of the September 11 intelligence failure is known, and longer still before a reliable account is available in public. Rather than recap the rumors and fragmentary evidence of exactly what intelligence did and did not do before September 11, this chapter focuses on ways in which intelligence should improve, and limitations of proposals for reform. Near the end it looks at what the long history of successful surprise attacks may tell us about how much intelligence can do.

Throw Money at the Problem

There are two main ways to improve intelligence. One is to loosen restraints on collection of information -- more on that below. The other is to raise the overall level of effort by throwing money at the problem. Yes, and to accept that the price will be much waste, a price more easily paid in wartime than in peacetime.

There have been misallocations of effort in the past, but there are no silver bullets that were left unused before September 11, no crucial area of intelligence that was neglected altogether and that a few well targeted investments could cure. There is no evidence, at least in public, that more spending on any particular program would have averted the September 11 attacks. The group that carried off the attacks had formidable operational security, and the most critical deficiencies making their success possible were in airport security and in legal limitations on domestic intelligence monitoring. In intelligence there is, however, a large number of areas in which efforts were extensive, but spread thin or slowed down.

It will take large investments to make just marginal reductions in the chance of disaster. Marginal improvements, however, can spell the difference between success and failure in some number of cases. If effective intelligence collection increases by only five percent for the year, but the critical warning indicator of an attack turns up in that five percent, spending a lot to gain a little information gains a lot of protection. Streamlining is a nice idea in principle, but risky unless it is clear what is not needed. When threats are numerous and complex, it is easier to know what additional capabilities we want than to know what we can safely cut.

After the Cold War, intelligence resources went down as requirements went up -- a whole new set of high priority issues and regions. At the end of the 1990s there was an uptick in the intelligence budget, but the system was still spread thinner over its targets than it had been when focused on the Soviet Union. Three weeks before September 11, Director of Central Intelligence (DCI) George Tenet gave an interview to *Signal Magazine* that seems tragically prescient. He agonized about the prospect of a catastrophic intelligence failure. "Then the country will want to know," Tenet warned, "why we didn't make those investments; why we didn't pay the price; why we didn't develop the capability."[2]

---

[2] Quoted in Robert K. Ackerman, "Intelligence at the Crossroads," Signal

The sluice gates for intelligence spending will open for awhile. The problem is not to buy some essential element of capability that was ignored before, but to help the system do more of everything, better. That will make the odds go up that bits and pieces of critical information will be acquired and noticed rather than falling through the sieve.

Collecting Intelligence

What can be improved easily will help marginally, while what could help more than marginally cannot be improved easily. The National Security Agency (NSA), National Imagery and Mapping Agency (NIMA), and associated organizations can increase "technical" collection -- satellite and aerial reconnaissance, signals intelligence, communications monitoring -- by buying more platforms, devices, and personnel to exploit them. To increase useful human intelligence -- what all agree is the most critical ingredient for rooting out secretive terrorist groups -- cannot easily be done by quick infusions of money.

Technical collection is invaluable, and has undoubtedly figured in previous counter-terrorist successes in ways thankfully not publicized. But obtaining this kind of information has been getting harder. For one thing, so much has been revealed over the years about U.S. technical collection capabilities that the targets now understand better what they have to evade. State sponsors of terrorism may know satellite overflight schedules time observable activities accordingly. They can utilize more fiber optic communications, which are much harder to tap than transmissions over the airwaves. Competent terrorists know not to use cell-phones for sensitive messages, and even small groups have access to impressive new encryption technologies.

Human intelligence is the key because the essence of the terrorist threat is the capacity to conspire. The best way to intercept attacks is to penetrate the organizations, learn their plans, and identify perpetrators so they can be taken out of action. Better human intelligence means bolstering CIA's Directorate of Operations (DO), the main traditional espionage organization of the U.S. government. The service has been troubled and periodically disrupted ever since the crack-up of the Cold War consensus in the late stage of the Vietnam War provoked more oversight and criticism than is congenial to spies. Personnel turnover, tattered esprit, and a growing culture of risk aversion constrained DO effectiveness.

Some of the constraint was a reasonable price to pay to prevent excesses when such organizations are subject to little scrutiny, and in a post-Cold War world where the DO was working for the country's interests rather than its survival. The weight of worries about excess receded after the collapse of the WTC, and measures will be found to make it easier for the clandestine service to move. One simple reform, for example, is to implement a recommendation made by the National Commission on Terrorism fifteen months before September 11 -- to roll back the additional layer of cumbersome procedures instituted in 1995 for gaining approval to employ agents with "unsavory"

Magazine (October 2001).

records, procedures that had a chilling effect on recruitment of the thugs appropriate for penetrating terrorist units.[3]

Building up human intelligence networks worldwide is a long-term project. It also inevitably spawns concern about waste (many such networks will never produce anything useful), deception (human sources are widely distrusted), and complicity with murderous characters (such as the Guatemalan officer who prompted the 1995 guidelines on recruitment). These are prices that can be borne politically in the present atmosphere of crisis. If the crisis abates, however, commitment to the long-term project could falter.

More and better spies will help, but no one should expect breakthroughs if we get them. It is close to impossible to penetrate small, disciplined, alien organizations like al-Qaida -- and especially hard to find reliable U.S. citizens who have even a remote chance of trying. Thus we usually rely on foreign agents of uncertain reliability. Despite our huge and educated population, the base of Americans on which to draw is small. There are simply few genuinely bilingual, bicultural Americans capable of operating like natives in exotic reaches of the Middle East, Central and South Asia, or elsewhere that shelter the Osama bin Ladins of the world.

For similar reasons there have been limitations on capacity to translate information that does get collected. The need is not just for people who have studied Arabic, Pashto, Urdu, or Farsi, but for those who are really fluent in those languages, and fluent in obscure dialects. Should U.S. intelligence trust recent, poorly educated immigrants for these jobs if they involve highly sensitive intercepts? How much will it matter if there are errors in translation, or willful mistranslations, that cannot be caught because there are no resources to cross-check the translators? Money can certainly help here, by paying more for translators and, over the long term, promoting educational programs to broaden the base of recruits. For certain critical regions of the world, however, there are not enough potential recruits waiting in the wings to respond to a crash program.

Intelligence Analysis

Money can buy additional competent people to analyze collected information more readily than it can buy spies who can pass for members of the Taliban -- especially if multiplying job slots is accompanied by enhancements of career development within intelligence agencies to make long service for analysts attractive. Pumping up the ranks of analysts can make a difference -- and within the relatively short time span of a few years. The U.S. intelligence community has hundreds of analysts, but hundreds of countries and issues to cover. On many subjects the coverage is now only one analyst deep -- and when that one goes on vacation, or quits, the account may be handled out of the back pocket of a specialist on something else. We usually do not know in advance which of the numerous low-priority accounts might turn into the highest priority overnight (for example, Korea before June 1950, or Afghanistan before the Soviet invasion).

---

[3] Countering the Changing Threat of International Terrorism, Report of the National Commission on Terrorism, Pursuant to Public Law 277, 105th Congress, June 2001, pp. 7-8.

Hiring more analysts will be a good use of resources, but there could turn out to be a low payoff -- perhaps none at all -- for much of what they do. Having a half-dozen analysts for some small country might be a good thing if that country turns out to be central to the campaign against terrorists, but those analysts need to be in place before we know we need them if they are to hit the ground running when we do need them. In most such cases odds are that those analysts would serve their whole careers without producing anything that the U.S. government really needs. Good analysts will not want to be buried in inactive accounts with peripheral significance.

One option is to make better use of an intelligence analyst reserve corps: people with other jobs who come in to read up on their accounts a couple days each month to maintain currency, and who can be mobilized if a crisis involving their area erupts. There have been experiments with this, but apparently without enough satisfaction to institutionalize a system more broadly.

Quantity of analysts is less important than the quality of what they produce. Post-mortems of intelligence failures usually reveal that very bright analysts failed to predict the disaster in question, despite their great knowledge of the situation. Or, they had warned that an eruption could happen, but without any idea of when. In fact, expertise can get in the way of anticipating a radical departure from the norm, because the depth of expert knowledge of why and how things have gone as they have day after day for years naturally inclines the analyst to estimate that developments will continue along the same trajectory. It is always a safer bet that the situation tomorrow will be like it has been for the past dozen years, than that it will change abruptly. In the vast majority of cases that prediction of continuity is absolutely correct; the trick is to figure out which case will be the exception to a powerful rule.

A standard recommendation for reform -- one made regularly by people discovering the problems for the first time -- is to encourage "out of the box" analyses that challenge conventional wisdom and consider scenarios that appear low in probability but high in consequence. To some, this is the sort of intellectual shake-up that might have led the intelligence system, rather than Tom Clancy, to anticipate the kamikaze hijacking tactic of September 11.

All well and good. The problem is figuring out what to do with the work this produces. There are always three-dozen equally plausible dangers that are improbable but possible. How should policymakers be convinced to focus on any of these hypothetical warnings or pay the costs of taking preventive action against them? One answer is to use such analysis to identify potential high-danger scenarios for which low-cost fixes are available. If President Clinton had gotten a paper two years before September 11 that outlined the scenario for what ultimately happened, he probably would not have considered its probability high enough to warrant an effort to revolutionize airport security, given all the obstacles of vested interests, opposition to particular measures, and irritation of the travelling public. He might, however, have pushed for measures to allow checking the rosters of flight schools and investigating students who seemed uninterested in take-offs and landings.

Another problem frequently noted is that the analytical corps has become fully absorbed in current intelligence, leaving no time for long-term research projects that look beyond the horizon. This too is something that more resources can solve. But as good a thing as more long-range analysis is (a

mission dear to the hearts of academic researchers like myself), it is uncertain how productive it will be for counter-terrorism. The comparative advantage of the intelligence community over analysts on the outside of government is in bringing together secret information with knowledge from open sources. The more far-seeing a project, the less likely is secret information to play a role in the assessment. No one can match analysts from CIA, DIA, or NSA for the task of estimating Osama bin Ladin's next moves, but what is their comparative advantage over Middle East experts in think tanks or universities for estimating worldwide trends in radical Islamist movements over the next decade? Such long-term research is an area where better use of outside consultants and improved exploitation of academia could help most.

Domestic Intelligence

There is a world of difference in the problems of collecting intelligence abroad and at home. All U.S. intelligence operations must conform to U.S. law. Abroad, however, they may break the laws of the countries in which they are undertaken. The clandestine service can bribe foreign officials, burglarize offices of political parties, plant bugs in defense ministries, tap the phones of diplomats, and do all sorts of things to gather information that the FBI could not do within the United States without getting a warrant from a court. Collection inside the United States is the area where loosened constraints would have done most to avert the September attacks. It is also where great changes may make Americans fear that the costs exceed the benefits -- indeed, that if civil liberties are compromised, "the terrorists will have won.".

A Minnesota flight school reportedly alerted authorities a month before September 11 that a student, Zacarias Moussaoui, was learning to fly large jets but did not care about learning to take off or land. Moussaoui was arrested on immigration charges, and French intelligence warned U.S. officials that he was an extremist. FBI headquarters nevertheless decided against seeking a warrant for a wiretap or search, reportedly because of complaints by the chief judge of the Foreign Intelligence Surveillance Court about other applications for wiretaps. After September 11 a search of Moussaoui's computer revealed that he had collected information about crop-dusting aircraft -- a potential delivery system for chemical or biological weapons. U.S. officials came to suspect that Moussaoui was supposed to have been the missing fifth hijacker on United Flight 93, which went down in Pennsylvania.[4]

With hindsight, the hesitation to mount aggressive surveillance and searches in this case -- hesitation linked to a highly developed set of legal safeguards rooted in the traditional American reverence for privacy -- is exactly the sort of constraint that should have been loosened. High standards for protecting privacy are like strictures against risking collateral damage in combat operations. Those norms take precedence more easily when the security interests at stake are not matters of one's own people's survival, but become harder to justify when they are.

---

[4] David Johnston and Philip Shenon, "F.B.I. Curbed Scrutiny of Man Now a Suspect in the Attacks," New York Times, October 6, 2001, pp. A1, B6; James Risen, "In Hindsight, C.I.A. Sees Flaws that Hindered Efforts on Terror," New York times, October 7, 2001, p. B2.

There have already been moves to facilitate more extensive clandestine surveillance, as well as reactions against going too far. There will be substantial loosening of restraint on domestic intelligence collection, but how far it goes depends on the frequency and intensity of future terror attacks inside the USA. If there are no more that seem as serious as September 11, compromises of privacy will be limited. If there are two or three more dramatic attacks, all constraint may be swept away.

It is important to distinguish two types of constraints on civil liberties. Political censorship, like the suppression of dissent in World War I, is one. There is no need or justification for this; counter-terrorism does not benefit from suppression of free speech. The second type involves compromises of individual privacy (through secret surveillance, monitoring of communications, and searches). This is where pressing up to the constitutional limits offers the biggest payoff for counter-terrorist intelligence. It also need not threaten individuals unnecessarily if careful measures are institutionalized to keep secret the irrelevant but embarrassing information that may inadvertently be acquired as a byproduct of monitoring. Similarly, there are popular but unpersuasive arguments against the sort of national identification card common in other democratic countries. The U.S. Constitution does not confer the right to be unidentified to the government.

Even modestly more intrusive information gathering will be controversial, but if it helps to avert future attacks, it will avert far more draconian blows against civil liberties. Moreover, Americans should remember that many solid humane democracies -- Britain, France, and others -- have far more permissive rules for gathering information on people than Americans have had, and seem to live with them without great unease.

Red Tape and Reform

In a bureaucracy, reform means reorganization; reorganization means changing relationships of authority; and that means altering checks and balances.

Five days after September 11, DCI Tenet issued a directive that subsequently leaked to the press. In it he proclaimed the wartime imperative to end business as usual, to cut through red tape and "give people the authority to do things they might not ordinarily be allowed to do....If there is some bureaucratic hurdle, leap it....We don't have time to have meetings about how to fix problems, just fix them."[5] That refreshing activism will help push through needed changes. Some major reorganization of the intelligence community is inevitable. That was the response to Pearl Harbor, and more than a half century after the National Security Act many thought it was time for a shake-up anyway.

The current crisis presents the opportunity to override entrenched and outdated interests, to crack heads and force consolidation and cooperation that have been inhibited by bureaucratic constipation. On balance reorganization will help -- but at a price. Mistakes will increase too. As Herbert Kaufman reveals in his classic little book, *Red Tape*,[6] most administrative obstacles to

[5] Risen, "In Hindsight, C.I.A. Sees Flaws...," p. A1.

[6] Herbert Kaufman, Red Tape (Washington, D.C.: Brookings Institution, 1977).

efficiency do not come from mindless obstructionism. The sluggish procedures that frustrate one set of purposes have usually been instituted to safeguard other valid purposes. Red tape is the warp and woof of checks and balances. More muscular management will help some objectives and hurt others.

The crying need for intelligence reorganization is no recent discovery. It is a perennial lament, amplified every time intelligence stumbles. The community has undergone several major reorganizations and innumerable lesser ones over the past half-century. No one ever stays satisfied with reorganization because it never seems to do the trick -- if the trick is to prevent intelligence failure. Will the next reform do better than the others?

Reorganizations usually prove to be three steps forward and two back, because the intelligence establishment is so vast and complex that the net impact of reshuffling may be indiscernible. After September 11 some observers complained that the intelligence community is too regionally oriented, and should organize more in terms of functional issues. This is reminiscent of the reverse frustration William Casey felt when he became Ronald Reagan's DCI and encountered the functional organization of CIA's analytical directorate. Rather than deal with functional offices of economic, political, and strategic research, each with regional subunits, he shifted the structure to one of regional units with functional subunits. Perhaps it was an improvement, but is there any evidence that it produced consistent improvement in analytical products? Will moving back in the other direction after September 11 help any more?

Or what about a better fusion center for intelligence on counter-terrorism, now touted by many as a vital reform? For years the DCI has had a Counter-Terrorism Center (CTC) bringing together assets from CIA's DO and DI, FBI, DIA, State, and other parts of the community. It has been widely criticized, but many believe its deficiencies came from insufficient resources -- something reorganization will not cure. If the CTC's deficiencies were truly organizational, is there good reason to believe that a new fusion center will not replace those problems with different ones?

Finally, some believe that the problem is the sheer complexity and bulk of the community, and that it needs to be streamlined, turned into a leaner and meaner corps. Few such proposals specify what functions can be dispensed with in order to thin out the ranks. In truth, bureaucratization is both the great weakness and great strength of the U.S. intelligence community. The weakness is obvious, as in any large bureaucracy: various forms of sclerosis, inertia, pettiness, and paralysis, which drive out many vibrant people and deaden many who remain. The strength, however, is taken for granted: a coverage of issues that is impressively broad, and for some, deep. Bureaucratization makes it hard to extract the right information efficiently from the globs of it lying around in the system, but in a leaner and meaner system, much will never be lying around.

Some areas can certainly benefit from reorganization. One is the integration of information technologies, management systems, and coordination of information sharing. Much has been done to exploit the potential of information technology, but it has been such a fast-developing sector of the society and economy in general that constant adaptation may be necessary for some time.

Another is in the long-standing tension over making the DCI's authority commensurate with his

responsibility, since roughly 80 percent of the intelligence establishment, in terms of functions and resources, has always been in the Defense Department, where primary lines of authority and loyalty run to the military services and to the Secretary of Defense. The latest manifestation of that problem was the increased priority given to the whole intelligence establishment in the 1990s for the mission of Support for Military Operations (SMO). This was odd, given that military threats to the United States after the Cold War were lower than at any other time in the existence of the modern intelligence community, while a raft of new foreign policy involvements in various parts of the world were coming to the fore. But the SMO priority was the legacy of the Persian Gulf War and the problems in intelligence support felt by military commanders, combined with the Clinton administration's unwillingness to override strong military preferences.

Matching authority and responsibility is where the test of the most immediate reform initiative -- or evidence of its confusion -- will come. Early reports on the formation of the Office of Homeland Security indicated that the new Czar, Governor Ridge, will be responsible for coordinating all of the agencies in the intelligence community. This is odd. That was precisely the function for which the office of Director of Central Intelligence was created in the National Security Act. The position of DCI was meant to centralize oversight of the dispersed intelligence activities of the military services, State Department, and the new Central Intelligence Agency, and to coordinate planning and resource allocation among them.

As the community burgeoned over the years, adding huge organizations like NSA, DIA, NIMA, and others, the DCI remained the official responsible for knitting their functions together. His ability to do so increased at times, but was always limited by the authority of the Secretary of Defense over the Pentagon's intelligence agencies. Indeed, hardly anyone but professionals within the intelligence community understand that there is a DCI. Not only the press, but presidents and government officials never refer to the DCI by that title, but always speak of him as the "Director of CIA," as if he is simply an agency head, forgetting the importance of the larger coordination responsibility.

Is Governor Ridge to become the central coordinating official in practice that the DCI is supposed to be in principle? If so, why will he be better positioned to do the job than the DCI has been? The DCI has always had an office next to the White House as well as at CIA, and Ridge will have to spend most of his time on matters other than intelligence. The real problem of DCIs in doing their jobs is that Presidents have hardly ever cared enough about intelligence to make the DCI one of their top advisers. Assigning coordination responsibility to Governor Ridge may work if the President pays more attention to him than he has to the DCI, but otherwise this is the sort of reform that could easily prove to be ephemeral or unworkable, yet necessary in the short term to tell ourselves that we are doing something significant.

Awake at the Switch and in the Dark: Surprise Attacks Will Often Succeed

The issue for reform is whether there is a cure to be found that can break a historic pattern. After September 11, intelligence officials realized that fragmentary indicators of impending action by

Osama bin Ladin's network had been recognized by the intelligence system but had not been sufficient to show what or where the action would be. A vague warning was reportedly issued, but not one that was a ringing alarm.[7] This is, sadly, a very familiar occurrence.

Even without the full inside story, we can understand much from looking at history. What we know of intelligence in conventional warfare does not answer some questions peculiar to terrorism, but it does help explain why powerful intelligence systems are often caught by surprise. The good news from history is that attackers often fail to win the wars that they start with stunning surprises -- Germany after invading the Soviet Union, Japan after Pearl Harbor, North Korea after 1950, Argentina after taking the Falklands, Iraq after swallowing Kuwait. The bad news is that those initial attacks almost always succeed in blindsiding the victims and inflicting terrible losses.[8]

Once war is underway, it becomes much harder to surprise the victim. The original surprise puts the victim on unambiguous notice. It shears away the many strong reasons that exist in peacetime to estimate that an adversary will not take the risk of attacking. It was easier for Japan to surprise the United States at Pearl Harbor than at Midway. But even in the midst of war, surprise attacks often succeed -- the Battle of the Bulge, the Tet Offensive. For Americans, September 11 was the Pearl Harbor of terrorism. The challenge now is to make the next attacks more like Midway than like Tet.

Surprise attacks often succeed despite the availability of warning indicators. This pattern leads many observers to blame derelict intelligence officials or irresponsible policymakers. The sad truth is that the fault lies more in organizational forces of nature, and in the pure intractability of the problem, than in the skills of spies or statesmen.

After surprise attacks, intelligence post mortems usually discover indicators that existed in advance, but were obscured or contradicted by other evidence. Roberta Wohlstetter's classic study of Pearl Harbor identified this as the problem of signals (information hinting at the possibility of enemy attack) getting lost in a crescendo of "noise" (the voluminous clutter of irrelevant information that floods in, or other matters competing for attention).[9] Other causes abound. Some have been partially overcome, such as technical limitations on timely communication, or organizational obstacles to sharing information. Others are deeply rooted in the complexity of threats, ambiguity of partial warnings, and the ability of plotters to overcome obstacles, manipulate information, and deceive victims.

One example is the "cry wolf" problem, in which the very excellence of intelligence collection works against its success. There are often numerous false alarms before an attack, and the false alarms

---

[7] Risen, "In Hindsight, C.I.A. sees Flaws...," p.B2.

[8] For surveys of numerous cases of surprise and its causes see Ephraim Kam, Surprise Attack: The Victim's Perspective (Harvard University Press, 1988) and Richard K. Betts, Surprise Attack: Lessons for Defense Planning (Brookings Institution, 1982).

[9] Roberta Wohlstetter, Pearl Harbor: Warning and Decision (Stanford University Press, 1962).

dull sensitivity to warnings of the attack that does occur. Sometimes the false alarms were correct warnings, but prompted responses by the victim that caused the attacker to cancel and reschedule his assault, thus becoming self-negating prophecy.

A variant is an overload of incomplete warnings, a particular problem for a superpower with world-spanning involvements. In the spring of 1950 CIA warned the President that the North Koreans could attack at any time, but without indications of whether the attack was certain or when it would happen. "But this did not apply alone to Korea," Truman noted in his memoirs. The same reports also continually warned him of many other places in the world where Communist forces had the capability to attack.[10]

Intelligence may correctly warn of the intent of an enemy to strike, and even anticipate the timing, but guess wrong about where or how the attack would occur. U.S. intelligence was warning in late November 1941 that a Japanese strike could be imminent, but expected it in Southeast Asia. Pearl Harbor seemed an impractical target because it was too shallow for torpedo attacks. That had been true, but shortly before December the Japanese adjusted torpedoes so that they could run in the shallows. (Similarly, before September 11, attacks by al-Qaida were expected, but elsewhere in the world, and not by the technical means of kamikaze hijacking.)

The list of reasons for surprise that are found repeatedly in post-mortems goes on. The point is that intelligence can rarely be perfect and unambiguous, and there are always good reasons to misinterpret it. Some problems of the past will not be problems for the technically sophisticated system we have now, and some may be reduced by adjustments of the system. But some cannot be eliminated.

Reorganization may be the proper response to failure, if only because the masters of intelligence do not know how else to improve performance. The underlying cause of mistakes in performance, however, lies not in the structure and process of the intelligence system. It is intrinsic in the issues and targets with which intelligence has to cope -- the crafty opponents who strategize against it, and the alien and opaque cultures which are not second nature to American minds.

Reform will happen and, on balance, should help. But for too many policymakers and pundits, reorganization is an alluring but illusory quick fix. Long-term fixes are vaguer and less certain, and reek of the lamp. But if the United States is going to have markedly better intelligence in parts of the world where few Americans have lived, studied, or understood local mores and aspirations better than Mohamed Atta and his colleagues understood ours, it is going to have to overcome a cultural disease. That is the disease of thinking that American primacy makes it unnecessary for American education to foster broad and deep expertise on foreign, especially non-western, societies. This is perhaps the only major country in the world where one can be considered well educated yet speak no other language but the native tongue. The disease has even infected the academic world, which should know better. American political science, for example, has driven area studies out of fashion. Some "good" departments have not a single Middle East specialist on their rosters, and hardly any at all have a

---

[10] Harry S Truman, Memoirs, vol. 2: Years of Trial and Hope (Doubleday,1956), p. 331.

specialist on South Asia -- a region of over a billion people, two nuclear-armed countries, and swarms of terrorists -- yet the same departments can afford a plethora of professors who conjure up models meant to apply globally. Reforms that can be undertaken now will make the intelligence community a little better, but to make it much better ultimately requires revising educational norms and restoring the prestige of public service. Both are lofty goals and tall orders, requiring general changes in society and professions outside government. Even if achieved, such fundamental reform will not bear fruit until far in the future.

The conservative tenor of this chapter is not a counsel of despair. To say that there is a limit to how high the intelligence batting average will get is not to say that it cannot get significantly better. It does mean, however, that no strategy for a war against terror can bank on prevention. Better intelligence may give us another several big successes like those of the 1990s, but even a .900 average will produce another big failure. That means that equal emphasis must go to measures for civil defense, medical readiness, and "consequence management," for blunting the effects of attacks that terrorists do manage to bring off. Prevention, and readiness for failure to prevent, go hand in hand.

OSS '02 PROCEEDINGS "The New Craft of Intelligence: Brainpower, Webpower, & Ground Truth" - Link Page

Previous	Dr. Max Manwaring
Next	GOLDEN CANDLE AWARDS

Return to Electronic Index Page