

Intelligence Test

Post-9/11 intel reform has been in name only. To make America safer, we need fundamental change across the entire government.

S

ince 2001, America's intelligence agencies have been doubly damned. First they were deemed incompetent for their failures on September 11 and for the infamous 2002 National Intelligence Estimate (NIE) on the Iraqi weapons of mass destruction that weren't, then they were tarnished by the epithets of scandal labeled "Guantánamo," "torture," and "spying on Americans." They thus face the challenge of reshaping themselves *and* restoring their social contract with the American people—in which the American people understand that they cannot know all the details of what intelligence agencies do in their name but require that those agencies respect the limits of American values—before they can become fully functioning tools for national security.

These failures have powered thousands of hours of hearings and thousands of pages of planning. But so far, the carousel of reorganization has produced more

GREGORY TREVERTON *is the director of the Center for Global Risk and Security at the RAND Corporation and author of the forthcoming Intelligence for an Age of Terror.*

shuffle than substance. To truly reshape intelligence gathering in order to meet today's threats, all of the Cold War legacy must be put on the table: organizations, security practices, and, especially, connections to U.S. society. As the intelligence community reshapes itself, and particularly as it needs to collect more information at home against a changed threat, it will confront a paradox: Domestic intelligence will be acceptable only with more transparency, but transparency can tip off would-be targets about how to stay below the radar. What is required are mechanisms for accountability and oversight to serve as surrogates for what the American people would find acceptable if they could only know.

Confronting a Changed Threat

Driving the reshaping of intelligence is the changing nature of the threat. The change can hardly be overstated. To be sure, some states, like North Korea or China or Russia, are still important targets for intelligence. But transnational targets, like terrorists or criminals, which were secondary before are now primary. The Soviet Union was a relatively bounded problem. It was glacial. It was not likely to surprise. The only surprise came when its glaciality became too onerous, and it collapsed suddenly. Cold War intelligence targeted big things with addresses, like Soviet armies, that weren't likely to change fast. Now, the priority is small things without addresses, which may change unpredictably as new groups or attack modes arise. September 11 drove home just how much damage a small group of determined men could do.

Three other differences are more consequential still. We had some "story" about states, even states as different from us as the Soviet Union. They were geographic, bureaucratic, and hierarchical. As a result, intelligence had a framework in which to locate new information, and communicating with policymakers was relatively easy because they shared the same frame. Even more important, in the old world of intelligence, the problem could be taken to be understanding "over there." While we hoped to influence Soviet behavior, we didn't expect that we would. So the challenge was understanding them on their terms. As former Secretary of Defense Harold Brown quipped about the U.S.-Soviet nuclear competition, "When we build, they build. When we cut, they build."

But terrorists are utterly different. They are constantly adapting to us and our vulnerabilities. The September 11 terrorists weren't airplane buffs; rather, they had done enough good tactical reconnaissance to know their plan would succeed. They had found the seams in our system. Today, it's not enough to know about them; intelligence can't understand them without knowing a lot about "us"—an especially uncomfortable fact for those agencies, like the CIA and NSA, which have long been enjoined from working on or in the United States.

Moreover, many intelligence questions about terrorists are “complexities,” not puzzles or mysteries. Puzzles have clear solutions. Mysteries are unknowable, but they have some shape; we know what variables matter most in producing an outcome, and we may have some historical evidence about how they interact. The Soviet Union was a puzzle: There was a lot we didn’t know, but we had a general idea of how things should look, and so as we found new puzzle pieces, we knew where to fit them. Complexities, though, are mysteries-plus. Large numbers of relatively small actors respond to a shifting set of situational factors—groups forming and reforming, seeking to find vulnerabilities, thus adapting constantly, and interacting in new ways. There may be no historical patterns in either what to look for or how the critical factors interact. Dealing with complexities in the new world of intelligence will require a dramatic rethinking.

The two intelligence failures of the early 2000s led to the creation of the Department of Homeland Security (DHS), which was mostly operational in intent, trying to produce some coherence among the various agencies responsible for protecting America’s borders and responding to internal disasters. For intelligence, there were three primary changes. First was the reorientation of the FBI’s mission. Second, the Intelligence Reform and Terrorism Prevention Act of 2004 set up the National Counterterrorism Center (NCTC), suggesting a new model for how intelligence did its work. Finally, that act also created the director of national intelligence (DNI) in an effort to build “jointness” across the 16 agencies of the intelligence community. All of these were steps forward, but all of them failed to change the nature of our intelligence structure, and so ultimately failed in improving our intelligence capabilities.

THE FBI

The 9/11 attacks prompted immediate calls to establish a new domestic intelligence service, separate from the FBI. The 9/11 Commission’s diagnosis pointed straight at the limitations imposed by the FBI’s culture of case-based law enforcement, saying that FBI agents were “trained to build cases, [and] developed information in support of their own cases, not as part of a broader more strategic [intelligence] effort.” Quite literally, while the Bureau did traditional counter-intelligence against the spies of foreign nations, in its primary law enforcement mission, if information wasn’t relevant to a criminal case at hand, it wasn’t considered worth saving. As a result, captured terrorist handbooks went untranslated. Likewise, sharing information, even with intelligence agencies, risked compromising existing cases, and so rarely occurred.

FBI director Robert Mueller, who had been in the post for one week on September 11, moved quickly to reorient the Bureau toward prevention and

intelligence; his reorganization plan reached Congress in November 2001. For counterterrorism purposes, he centralized the Bureau's famously autonomous field offices. As Arthur Cummings, now head of the National Security Branch, explained, for today's Bureau, "There is no such thing as a local terrorism problem. Something might happen locally, but within two seconds, you discover national and international connections." The Bureau's website advertises its top priority as "protect[ing] the United States from terrorist attack." The FBI's budget more than doubled between 2001 and 2008, from \$3.1 to \$6.4 billion. It increased from 34 to 101 the number of joint terrorism task forces (JTTFs), which bring together FBI agents, state and local law enforcement officials, and representatives from other federal agencies to investigate terrorism cases.

This transformation is indeed a sea-change. When I oversaw NIEs in the 1990s, I knew the FBI through intelligence, but that was like trying to understand the National Football League by talking to the placekickers: Intelligence was important to the Bureau, but not central. It was labeled "support" (if not "furniture"), and the label was apt. Intelligence then meant mostly operational support: can you find this suspect's address? Now, the Bureau is trying to make intelligence-led prevention its mission across the organization. Those cases that earlier constrained what information was collected are meant to become, instead, platforms for collecting intelligence. It is an impressive goal and a revolution in organizational culture.

But does it work? In 2005, as part of its reconfiguration, the Bureau put its beefed-up Office of Intelligence back together with Counterintelligence and Counterterrorism in the National Security Branch (NSB), thus creating an intelligence branch with a similar relationship to the DNI as that of the NSA—i.e., not managed day-to-day by the DNI, but looking to that office for a budget and broad guidance. In effect, the FBI created a service-within-a-service.

On the plus side, this shows the FBI really does value intelligence work, a big change from before. The bad news is that while the counterterrorism squads think the work is important, they often do not like it. It is relentless, chasing one lead after another, without the closure of arrests. It's not what many in the Bureau signed up for. In short, the Bureau has changed, but that change is still very much a work in progress.

For now, Congress and the body politic have decided that Mueller and his colleagues deserve time to see if they can reshape the Bureau. Another major

The American intelligence community, having broken down earlier this decade, has been diagnosed and dismantled. It has not been rebuilt.

terrorist attack on the United States, however, would raise the question of whether the Bureau really could transform or if, instead, the nation required a new domestic intelligence agency.

THE NATIONAL COUNTERTERRORISM CENTER

The most far-reaching proposal made by the 9/11 Commission was to suggest that the intelligence community emulate the military's combatant commands, and the 2004 Act embodied that idea in the creation of NCTC. On this logic, the existing agencies—the CIA, the Defense Intelligence Agency (DIA), and the NSA, among others—would become, like the military services, responsible for building the intelligence forces, but those forces would be deployed by “national intelligence centers,” which would be shaped by issue or mission, rather than by organization or the source from which data was collected.

In the Cold War legacy of U.S. intelligence, collection was organized around information sources, while analysis was organized by agency. The big collectors were the CIA for espionage or human intelligence (HUMINT), NSA for signals intelligence (SIGINT), and the National Geospatial Intelligence Agency (NGA) for imagery (IMINT). In analysis, the CIA was the first among equals, but DIA was at least as large, and the processors and analysts at the big collectors, NSA and NGA, even larger in numbers. State's Bureau of Intelligence and Research (INR), only several hundred strong, punched above its weight in inter-agency arguments, and smaller intelligence shops existed in agencies all over Washington.

This pixilated configuration made some sense when the intelligence community had one over-arching target, the Soviet Union. There were also relatively few consumers of intelligence material. Pride of place was given to secret sources, which intelligence agencies “owned.” In effect, the collectors were asked: What can you contribute to understanding the puzzle of the Soviet Union? It worked, more or less, but it's no longer the right prescription. Not only have targets multiplied, but so have consumers, extending in principle to the 18,000 police jurisdictions in the United States which are potential partners in the fight against terrorism.

Thus the new structure, organizing by problem or mission on the model of the military's unified commands. In Iraq, for instance, Central Command (CENTCOM), the regional command for the Middle East region, managed the war, but the troops were provided by the military services, which executed operations under CENTCOM's direction. By analogy, the NCTC is to be the “unified command” in the war on terrorism, carrying out intelligence analysis and planning operations, while the CIA and other agencies provide the

analysts and other personnel and conduct the required operations, such as intelligence gathering.

To say the idea was not wildly popular with the existing agencies would be an understatement. They resisted thinking of themselves as force providers; they regard themselves as the doers. Well before 2004, agencies expressed concern about “center-itis,” the rise of specialized or issue-oriented groups within intelligence, like the CIA’s Counterterrorism or Counter-Narcotics centers. Agencies tend to think of personnel assigned to those centers as having been lost to the real work, back home at their agency. Changing that view to regard the real work as done by the centers, with the agencies in a supporting role, will require yet another sea-change in organizational culture.

The less parochial concern is that centers would be very much inclined to focus on the hottest current issues and would tend to produce worst-case analyses. These are serious matters. The military’s combatant commands do tend to have short time horizons and to worry about worst cases, for understandable reasons: If war broke out today, they would have to fight it. In a similar way, the centers would be the first ones blamed if crises developed without warning, and their plans would be the first ones exposed if remedies failed. So the bias toward current intelligence and the dramatic over-warning that now afflict all of U.S. intelligence—a theme that runs through the WMD commission report— could get worse.

So far, given the resistance of the existing agencies, NCTC is the closest U.S. intelligence has come to deviating from the usual way of doing business. Neither John Negroponte, the first DNI, nor Michael McConnell, his successor, pushed the center concept. In effect, NCTC became the “campus” for a confederation, collocating several hundred officials from the CIA Counterterrorism Center (CTC) and the FBI Counterterrorism Division (CTD), plus smaller numbers from other agencies, at its headquarters at Liberty Crossing near Tyson’s Corner, Virginia, not far from the CIA’s Langley headquarters.

In addition to connecting the dots, NCTC is to do “strategic operational planning,” a strange locution. In other words, it is caught somewhere between the past and the future. It was set up neither to execute operations—those were left to the agencies—nor to make policy, which would be left to the president and the National Security Council. It was to assign responsibilities for operations to lead agencies but not direct the execution of those operations. The conception of the NCTC is rooted in the understanding that the counterterrorism mission is intelligence rich and thus that planning needs to be intelligence driven. Yet the reach of NCTC planning into the operations of the major agencies, especially the military, remains uncertain. In effect, the American intelligence community,

having broken down earlier this decade, has been diagnosed and dismantled. It has not, however, been completely rebuilt. Given the continuing threat of terrorist attacks, it is a project the next president needs desperately to complete.

THE DIRECTOR OF NATIONAL INTELLIGENCE

The third intelligence reform, the creation of the DNI, got the most attention. The DNI was to have real power over the community, not just titular control, as the old Director of Central Intelligence (DCI) structure did. But this wasn't a new proposal, nor was it clear that DCIs actually lacked real power. In the Carter Administration, DCI Admiral Stansfield Turner exercised considerable control over the entire intelligence budget, and he built a serious program analysis staff to assist him.

Nevertheless, the 2004 Act did explicitly grant the DNI more authority than had been available to the DCI. But the rub is that, in the words of the WMD commission, the law gives the DNI "broad responsibilities but only ambiguous authorities." The job is more a hunting license than a full mandate. The DNI does prepare the National Intelligence Program (NIP)—that is, the broad budgets for all 16 national intelligence agencies—and appoints the director of the CIA subject to Senate confirmation. Predictably, the sticking point has been the exact power of the DNI over intelligence operations located in the Defense Department, especially the big technical collectors (NSA, NGA, and the National Reconnaissance Office). These agencies account for the vast bulk of the \$40 billion-plus national intelligence budget, and no secretary of defense had been eager to cede authority over them to the DCI—or the DNI.

The DNI is also hampered by having not one but two major demands on his time: He is the principal intelligence advisor to the president and strategic manager of the community. Negroponte emphasized the first, taking over control of managing and delivering the crown jewel of analysis, the President's Daily Brief (PDB), which had been the CIA's product; McConnell, a career military intelligence officer and former NSA director, continued the practice. Almost no one in Washington ever turns down face time with the president, but it is hard to overstate the time demands associated with overseeing and delivering the PDB. The DNI's subordinates lament that he hardly has time for anything else while he waits outside the Oval Office and works on his Blackberry.

McConnell sought to pick up the pace of reform with a 500-day plan emphasizing jointness among intelligence agencies. Yet a small example drives home the resistance the DNI faces from that mislabeled "community": In 2006, the DNI's office inaugurated a course known as Intelligence Analysis 101. It was to be for new analysts across the community, a small step toward jointness: Wouldn't it be

good for analysts in one agency to have some inkling of how their counterparts in another did their work? But even this idea was resisted by the various agencies, on the grounds that it undermined their separate “branding” and, slightly bizarrely, that it might lead to “groupthink.” In short, the DNI office has yet to do much in terms of creating a true intelligence “community”—precisely the reason it was created in the first place.

Changing the Way Intelligence Works

Multiple new threats and multiplying consumers require putting all the old distinctions on the table. Just as the terrorist threat is one for both intelligence and law enforcement, it does not respect any distinction between “here” and “there,” between foreign and domestic. Cold War intelligence drew a line between collector and analyst, and an even sharper one between intelligence and policy, lest intelligence be tainted (“politicized”) by too close an association with policy-makers and their agendas. Yet collectors and analysts increasingly merge, most visibly when someone searches the Web. That job of collection has to be done by people who know what they’re looking for—in short, analysts. And America’s challenge now is not framing policy with regard to a relatively predictable foe; rather, it is trying to make sense of a changed and unpredictable world. That task, ideally, needs to be undertaken by intelligence and policy in tight partnership. For the second time since September 11, we must re-imagine how intelligence works.

To some extent, this is starting to happen. One area where innovation has begun in recent years is changing the intelligence paradigm. The Cold War also drew a sharp distinction between public and private, nowhere more sharply than in intelligence, where the concentration on secret sources compounded the separation. Yet in the world before us, while secrets still count, much of the information and expertise is out there in the world, not in the intelligence agencies.

That was driven home to me a decade ago when I was managing the NIE process. The U.S. military’s Transportation Command requested an NIE or similar paper on future humanitarian emergencies, on the simple logic that it would be the deliverer of assistance and thus might ask in advance whether likely hardship locales had airstrips or seaports. The people who knew most about this issue were not in intelligence but rather in CARE and the other humanitarian non-governmental organizations (NGOs). So we asked them to come to a conference and bring a two-page paper. They didn’t especially like the idea of such a close collaboration with government, let alone intelligence, but what overcame their resistance was the fact that we were interested in their issue. They all came, their papers in effect writing the first draft of the estimate.

To that end, the DNI recently created an Open Source Center to take advantage of intelligence “out there.” The idea is hardly a bad one, but it still bespeaks the old categories. Intelligence still treats the entire information world beyond secrets as another “INT,” in this case OSINT, or open source intelligence. Yet as former CIA deputy director John Gannon put it, “Open source is not an INT, it’s the air they [the other INTs] breathe.” Other initiatives are promising but still timid—and far from sure to happen. One CIA proposal, unhappily stuck with the moniker iD8, would approach hard intelligence problems much as my own institution outside government, the RAND Corporation, does: It would first reach out to outsiders in academia, think-tanks, and Wall Street. It would work at the unclassified level, only classifying the work if it absolutely had to.

The fundamental challenge is to reshape how intelligence agencies think of information, and how it should be produced, used, and controlled.

Organizing by problem or mission, rather than information source or analytic agency, is a start toward breaking down the distinctions, especially that between collector and analyst. Perhaps, if the centers were seen as one-stop shopping, they could begin to break down that between intelligence and policy as well. A real re-imagining, however, would recognize that corporations and NGOs might be intelligence’s sources one day but customers the next, and fellow analysts all along. It would seek to restructure security and conflict-of-interest regulations to make it easy for people to move in and out of intelligence.

On the collection side, that re-imagining would break down those big collection baronies labeled in government-ese “stovepipes” or “silos”—SIGINT, IMINT, and HUMINT—and dominated on the technical side by satellite platforms. The process would start with hard questions about what information the government needs to make and what it can buy (or have for free). Already, pretty good imagery is available on the Web, as anyone who’s looked for their house on Google Earth knows. NRO was a creative satellite builder in its day, but that day has passed, and so it should be supplanted by a new R&D organization that would ask for information that can’t be bought—not “how can a satellite collect that information?” but rather “what’s the best way to collect that information?” In all these ways, the fundamental challenge is to reshape how intelligence agencies, and the government in general, think of information, and how it should be produced, used, and controlled.

The intelligence community is also taking tentative steps in the right direction toward real inter-agency cooperation, work that can and should be built upon.

The FBI JTTFs are a step towards that end; so too is a newer and promising DHS initiative, “fusion centers.” These are intended to complement the JTTFs, which work on cases once identified, by assembling strategic intelligence at the regional level. They too seek to bring together federal, state, and local officials, and to involve the private sector. The fusion centers face enormous challenges of organizational culture: In Los Angeles, for instance, it is hard enough to get the police department and county sheriff’s office to work together, let alone get the two of them to work easily with federal agencies. But it is a start.

Yet the ultimate challenge is conceiving the problem correctly. The goal is not just a two-way street for data, but rather jointly producing useful information across the far-flung American federal system. It is what John Sullivan of the L.A. sheriff’s office calls, with perhaps just a hint of Hollywood, “co-production.” That would put a premium on federal intelligence analysts first doing their work at a level than can be shared, not with all the bells and whistles of classification. It would build on comparative advantage: Local police have shoes on the ground but, except for the big departments—with New York in a category by itself—not much capacity to do analysis or specialized intelligence collection. Those cops on the beat can be eyes and ears in the fight against terrorism if they know what to look for and if they get something of value back when they report information to the feds.

Rebuilding Trust

Because intelligence agencies operate in secret and because they engage in activities that are sensitive or even illegal at home, they depend on public trust. I first came to know intelligence in the 1970s as a staff member of the first-ever Senate investigation of intelligence—usually called the Church Committee after its chair, Idaho Democratic senator Frank Church. The committee was formed when that trust had been broken by revelations about excesses both foreign and domestic, ranging from assassination plots against foreign leaders, to the covert CIA role in Chile and other countries, to illegal spying on Americans. Then, there were serious calls to abolish the CIA.

The contract is broken again. Even if the failures, like that of September 11, were the result of earlier decisions—like erecting a wall between intelligence and law enforcement—taken for good reasons, they were still failures. And even if the scandals, like Abu Ghraib or waterboarding, are at the margins of intelligence proper, they still cast a dark shadow over it. The outrages at Abu Ghraib were committed by military intelligence officers, and if interrogation was but a small part of Cold War strategic intelligence, it always has been a key element of police work and will be important to intelligence in an age of terrorism, both at

home and abroad. Intelligence agencies labor under the weight of having been deemed not just incompetent but malignant.

The simplest way to diminish the overhang of the scandals for intelligence is to end the practices that give rise to them. Rather than vetoes, an administration could start by stating that the United States categorically does not engage in torture, including waterboarding, and that no techniques other than those outlined in the Army Field Manual will be employed. It might underscore its seriousness by seeking, not shunning, congressional action in support of that view. It shouldn't be a close call: Even if it was waterboarding that eventually broke several high-value detainees like Khalid Sheikh Mohammed, Abd al-Rahim al-Nashiri and Abu Zubaida, the price was too high. The conflict with Islamic extremist terrorists is ultimately a war of ideas, and we lose the war if we stoop to their methods.

The change in intelligence's targets and the consequent need to expand surveillance at home require rethinking how intelligence activities are authorized and overseen if the contact is to be mended. There, too, the Cold War's solutions may no longer suffice. After the investigations of the 1970s, Congress passed the Foreign Intelligence Surveillance Act (FISA) to provide some judicial oversight of domestic surveillance for purposes of national security (as opposed to law enforcement). A secret court reviewed applications from Justice and the FBI. After September 11, however, the administration argued it could not target named individuals with specific warrants before the fact; rather it needed to scan wide swathes of communication, searching for connections of interest.

There is surely something to the argument that oversight will have to move from judicial approval before the fact to some form of continuing legal or congressional review as surveillance proceeds. Yet by overreaching and simply bypassing FISA, rather than working with Congress to try to fix it in the first years after September 11, the Bush Administration discredited good arguments for thinking about new procedures.

In his confirmation hearings, Supreme Court Justice Samuel Alito gave new salience to Justice Robert Jackson's distinction of a half-century ago: The president's power is greatest if his action is consistent with what Congress has done, less if Congress has been silent, and least if the action is contrary to the will of Congress. In passing FISA, Congress could hardly have been clearer. Not only did it make FISA "the exclusive means by which electronic surveillance... may be conducted" for national security purposes, it rejected the idea, discussed the Ford Administration, that would have left open the possibility that a president could continue warrantless taps, like those the Bush Administration engaged in after September 11.

INTELLIGENCE TEST

By all accounts, the FISA process is detailed and scrupulous—indeed perhaps too scrupulous in the case of Zacarias Moussaoui, the famous “20th hijacker” of September 11. Agents at the FBI’s field office in Minneapolis desperately sought to search his computer after he was arrested on a visa violation but were denied permission when FBI and Justice lawyers wrongly believed that existing FISA guidelines did not permit it. FISA requests are almost never formally rejected by the court, but that is because they are carefully crafted and sometimes withdrawn during the process.

The problem is that the process isn’t, and probably can’t be, very transparent, and the July 2008 law reforming FISA doesn’t go nearly far enough in providing independent oversight of NSA eavesdropping. The NSA is now allowed to seek court orders for broad groups of foreign targets, and the law creates a new seven-day period for directing wiretaps at foreigners without a court order in “exigent” circumstances if government officials assert that important national security information would be lost. The law also expands the period for emergency wiretaps on Americans without a court order, from three days to seven, if the attorney general certifies there is probable cause to believe the target is linked to terrorism. The law does make FISA the “exclusive” way of conducting intelligence eavesdropping, but it provides no explicit requirement that NSA return to the court to justify continuing surveillance, perhaps on just a subset of the original group.

Reshaping U.S. intelligence and rebuilding the social contract must go hand in hand. If the intelligence structure is not trusted, it will not be given the authority it needs to be effective in meeting the challenges of the new world. To change, it will have to both collect more information on private citizens at home and reach out to those citizens as collaborators. The latter means interacting with American society in dramatic new ways. It means opening up. Precisely because intelligence tools of the fight against terror cannot be entirely transparent, lest the nation’s enemies adapt their operations to circumvent them, the social contract requires some processes of secret oversight. The public doesn’t need to know the details of what is being done in its name. It does need to know that some body independent of an administration does know and does approve. What is critical is process before the fact and oversight afterward, if not before. If, in the famous phrase, the Constitution is not a suicide pact, neither is war a blank check. ▀