

A Perspective on Intelligence Reform

By Charles S. Faddis

Several years ago, while I was working operationally overseas, a team of analysts visited our office from headquarters in Washington, DC. These officers were on a tour of the region, and one of them offered to give a briefing to our local personnel regarding a terrorist group active in the country to which I was assigned and on which a lengthy piece of finished analysis had just been completed. The briefer, who had written the analysis, had reached a number of very interesting conclusions concerning the evolution of the group and believed that he was able to make a number of very detailed predictions regarding the direction this group would take in the future. Among other things, he was convinced that the group was losing support, was unable to maintain its previous level of activity and was likely to decline precipitously in significance in the months and years ahead. It was, in his opinion, no longer a serious threat to American interests. The briefing was well done, tight, focused, and, unlike so many such presentations, captivating.

It was also absolutely wrong.

I had run many of the sources which had produced the intelligence on which this analysis was based. I knew that the only thing that had changed regarding this group was our access. Where once we had significant detail on the internal workings of the terrorist organization in question, and a clear understanding of the complexity of its operations and the breadth of its capabilities, we were now slowly going blind. The group had not evolved. It was not losing support. We were simply unable to maintain access. The danger from this group was not declining. It was increasing.

It was a stark reminder of an obvious but frequently forgotten truth. You cannot analyze information you do not have, and your analysis is only as good as the intelligence on which it is based. You can listen to rumors, draw inferences from tiny snippets of information, and extrapolate from other known cases all you want. In the end, if you do not have hard facts, you are guessing, and, as events over the last many years show, in the business of terrorism you are often guessing wrong.

Seven years ago an al-Qaeda terrorist attack on U.S. soil killed roughly three-thousand Americans. Any number of American agencies and departments failed miserably in the discharge of their responsibilities on that occasion. First and foremost, 9/11 was a failure on the part of the Central Intelligence Agency (CIA). Put simply, we did not have the sources inside al-Qaeda we needed to warn us of the coming attack. Just as it had been on so many prior occasions, the U.S. was caught flat-footed and dealt a staggering blow. This time, however,

the impact was that much greater in that the attack occurred on U.S. soil and the death toll was enormous.

In the wake of these attacks and the subsequent intelligence errors concerning WMD in Iraq, the United States Government instituted a whole raft of “reforms” within the American Intelligence Community (IC). The most notable of these was the creation of an office of Director of National Intelligence, the DNI, who was charged with the task of coordinating the activities and budgets of the numerous separate intelligence agencies, which make up the IC. Whether or not he has the power to do this task remains to be seen. It should be remembered that prior to 9/11 there already was an individual, the Director of the CIA, whose job it was to run the IC. That he failed completely to direct and coordinate the activities of this sprawling community, which is overwhelmingly under the direction of the Pentagon, was directly attributable to the fact that he had no substantial authority to back up what was in reality a largely symbolic position.

In like fashion, all sorts of other changes and “reforms” were rolled out across the IC. Additional layers of bureaucracy were added in many organizations. New procedures were implemented with the goal of ensuring wider distribution of sensitive information both within the IC and to local law enforcement. Some of these made sense and were long overdue. Many of them had nothing to do with the problems at hand and were a reflection of the fact that bureaucracies and bureaucrats, left to their own devices, will always do what they do best. They will create rules, procedures and regulations.

Nothing in any of this addressed the most significant issue: the failure of the CIA to collect the human intelligence required to have provided advance warning of the pending attacks. The fact remained that the CIA, the United States’ premier intelligence organization, for a variety of reasons which I will delineate, remained incapable of performing its primary mission and safeguarding the nation it served.

The CIA is crippled by a whole host of ailments. Some of the wounds are self-inflicted. Many of them are not. None of them are curable by the addition of more bureaucracy and yet more layers of supervision, coordination and oversight. Meetings, PowerPoint presentations and long term strategic plans penned by individuals who have never met a terrorist and would not know one if they tripped over him do not produce intelligence reports.

The CIA, which began life once long ago in the mists of time as a band of bold, aggressive, highly creative individuals called the Office of Strategic Services (OSS), has become a stiff, rigid, overly bureaucratic structure dominated not by risk takers and rule breakers but by cautious, ladder-climbing bureaucrats. It has, in short, lost what made it special and capable of doing the impossible and transformed into just another plodding federal agency. In this context, therefore, all changes and “reforms” which add yet more bureaucracy and more “drag” take us not toward a solution but in exactly the wrong direction.

What exists as the CIA today is largely a product of the Cold War. It is a structure designed to collect information within the context of a long, largely static strategic struggle. It uses as its primary collection mechanism officially covered officers assigned abroad and targets mostly foreign officials. In the context of a worldwide confrontation with the Soviet Union, which lasted for decades, this structure generally made sense. It allowed the United States to place large numbers of personnel abroad, relatively quickly and cheaply, and it positioned those officers to work against their adversaries, Soviet intelligence and their allies.

Such a structure makes no sense whatsoever given the primary targets against which the organization is required to work today. If I am serving under official cover in a Third World country today, I am likely in a good position to make contact with local officials, with prominent members of the business and academic communities and to focus on other officials from nations hostile to American interests. My status as an American official, however, will be of no value whatsoever in gaining me access to members of terrorist groups, individuals involved in the smuggling of radiological material or drug cartels. At best, my status in the country will be of no help at all. To the extent I am required to live and work in true name and attract attention to myself via my official duties, my cover may, in fact, be a great hindrance.

Just as important as the structure of the organization, however, is its culture and its philosophical approach to risk and the conduct of operations. An agency built to collect long-term strategic intelligence via officially covered officers placed abroad develops a certain approach to risk taking. The emphasis is placed on the avoidance of a “flap”, a diplomatic incident. Operations which have the potential to turn ugly or to go wrong are avoided and the risk versus gain analysis is heavily weighted toward eliminating risk. If it comes to a choice between running an operation (op) or making sure that nothing goes wrong, the op is likely not to be run. There will always be time later to come back and make another attempt at collection. Threats are thought of as distant and slow in evolution.

Over time this approach becomes embedded in the culture of the organization. Officers are not routinely subjected to physical risk. They understand that, if caught, they may be questioned briefly, but the worst that will happen is that they will be sent home prematurely. They come to accept this as a way of life, and, gradually, they come to regard any level of risk beyond this to be unacceptable. An operation which has the potential to lead to the capture or death of a staff officer is simply considered “too risky”.

This focus on risk avoidance has been intensified by the political pressures on the CIA. Again and again, the President of the United States has called upon the CIA to conduct activities which were not supported by the Congress. In some cases, such as the Iran-Contra affair, these activities were, in fact, conducted contrary to explicit legislative prohibitions. When uncovered, these activities have provoked vicious Congressional responses, and significant numbers of CIA officers have either been forced into early retirement or prosecuted as a result.

Congress for its part, while entrusted with oversight authority, has chosen to focus more on making political hay out of CIA mistakes than it has on constructive engagement. Agency officers routinely find themselves being used as pawns in a power struggle between the Executive and Legislative branches of the United States Government. The result is predictable. Career officers, with spouses, children, mortgages and college expenses to think about keep their heads down, choose the safe route and avoid pushing the envelope.

During the Cold War the consequences of these problem were often less apparent. When you are trying to collect information on Soviet missile forces within the broader framework of a worldwide generational conflict, taking the long, patient, safe approach is, after all, usually wise. Unfortunately, it makes much less sense within the context of a fast moving, global war against a vicious enemy determined to strike, not a decade from now, but next week.

For this kind of conflict a very different approach is needed, one which emphasizes creativity, daring and imagination over deliberation and caution.

In essence, what is needed is an approach much like that which the original OSS utilized. While the OSS had a nominally military structure, it was a civilian organization and it employed a wide, eclectic mix of individuals ranging from paratroopers and Army officers to actors, professors and professional sports players. It also drew from the full cross-section of American society including in its ranks members of some of the oldest and most prominent families in the nation as well as recent immigrants still fluent in the tongues of their native lands.

The result was a free-wheeling organization staffed by what its leader William Donovan referred to as his “glorious amateurs” and characterized by what he described as “discipline daring”. Nothing was too novel or risky to be considered. The only thing that was absolutely unacceptable was a lack of movement. Donovan could accept failure. He could not accept inactivity. In his words, “If you fall, fall forward.”

The OSS understood precisely the level of risk which would have to be accepted in order to acquire the intelligence the nation needed. It posted officers abroad under a host of covers. Sometimes they operated as singletons, sometimes as armed teams working with local partisans. They were driven always, however, by the same dynamic: to do whatever was required to collect the needed intelligence. In many cases, this meant sending staff officers into occupied territory where they lived and worked undercover for months or years at a time stealing German, Italian and Japanese secrets. A significant number of these officers were caught, and many died a horrible death, but the OSS continued to do whatever it took to complete the mission. It did not relish the death of officers in the line of duty, but it understood that it was the inevitable cost of success.

This attitude and approach were not necessarily unique to the OSS. The British Special Operations Executive (SOE), for example, on which much of the OSS was patterned, shared a similar approach. Regulations and procedures were not regarded with much favor. Results were.

In the case of the OSS, those results were staggering. An organization which was created in 1942 was by war’s end in 1945 operating worldwide and running sources under the most extreme circumstances imaginable from the heart of the Third Reich to the jungles of Burma. The conditions under which the organization operated were often brutal, but, despite this, the organization forged ahead, and the United States acquired the intelligence it needed to win the Second World War.

Just as the OSS’s approach to intelligence collection was not necessarily unique, so too are the problems the United States faces in the collection of human intelligence not unique either.

The United States has been struck by terrorists without warning over a period of many years, beginning in Lebanon in the 1980s and culminating on September 11, 2001. Other nations have endured and continue to endure their own intelligence failures: the Madrid train bombings, the London underground bombings, the Beslan school massacre and a long list of at-

tacks in India perpetrated by Pakistani militants and their supporters. It has, in fact, become commonplace that terrorists strike without warning and that civilized nations are left to focus on managing the after effects of the event and deliberating regarding retaliation.

We have come to think of this as inevitable. It is not. The fact that intelligence agencies using current methodologies are not collecting the information that we need does not mean that it is impossible to collect this information. It does mean, however, that we are going to have to change our methodologies in order to achieve success. Approaches evolved to gain access to information on the strategic plans of hostile governments are not likely to prove useful in helping us get inside of small, highly compartmented organizations composed of brutal fanatics. For that task, we are going to have to go back to an approach which accepts as a given a level of risk much higher than that we have been tolerating and which employs techniques more in tune with those used to penetrate organized crime syndicates and drug cartels than those of the classic Cold War espionage cases.

Officers may still be placed abroad under official cover when this makes sense. More frequently, however, we are going to have to move to a system of placing officers overseas without the benefit of any official status. They will need to live and work in the milieu they are expected to penetrate. Their lives, when posted abroad, may be more analogous to those of Bureau of Alcohol, Tobacco, and Firearms (and Explosives) agents penetrating motorcycle gangs in the United States than they will to those of current officially covered intelligence officers. This will afford them much greater natural access to targets of current interest, but it will also mean that they will be subjected to much greater risk and that we will have to accept that level of risk to operate.

As noted earlier, if I am an intelligence officer serving abroad under official cover, and I get caught in the act of violating local laws, I am likely to be held for a short period of time, declared *persona non grata* and then sent home. It may not be the best day I ever had, and it may mean a great deal of disruption for my family, but I will survive.

Once we step across the line and begin to place significant numbers of officers abroad without the benefits of official cover and ask them to penetrate violent terrorist groups and organized crime cartels, we are entering an entirely different world. Now if I am caught, it is likely that I will die. That death may well be slow, painful and horrifying. The first notice that my home office has of a problem may be that my body is found by the side of the road downtown.

This is not glamorous. It is not pretty. It is not easy. It will require not only an acceptance of this kind of risk on the part of the organization, but also on the part of the individual officers called upon. It will also, frankly, call for a cadre of tough, well-trained and very disciplined operatives, who have been brought up from the point of their induction into the organization to cope with these demands.

That said, I would submit that we have no choice but to move in this direction. The failure of the United States Government and other allied nations to focus on the necessity for reform in the collection of human intelligence has had massive negative consequences to date. Continued inaction may well prove to be infinitely more damaging.

The world around us is evolving at a phenomenal pace. In many parts of the world the artificial “order” imposed by nation states that are largely the creation of former colonial powers is disintegrating. Lawless areas which hold the potential to serve as safe havens for terrorist groups appear with ever increasing frequency. We may or may not succeed in keeping Afghanistan from reverting to its role as a base for terrorist operations. Meanwhile, much of the Northwest Frontier Province is already serving as the de facto headquarters for al-Qaeda and Somalia is spiraling yet again into total chaos. Absent a miracle, the bulk of that war-ravaged nation will once be under the control of Islamic extremists within months.

Given the pressures of over-population, energy and water shortages, unemployment and religious fanaticism there is no reason to think this situation will improve anytime soon. We are living in a world which for the foreseeable future will include large, ungoverned areas wracked by tribalism, violence and extremism. These will be the base camps for terrorism for a long time to come, and if we are going to prevent future attacks we are going to have to field intelligence services which are capable of grappling with the organizations bred in such areas.

Nor is the nature of the attacks we face likely to remain static. While significant portions of the globe seem to be unraveling, the pace of technological advancement continues to quicken. Pakistan may be on the brink of implosion, but it’s still possible for a scientist in Peshawar operating with limited resources to do a credible job of creating both biological and chemical weapons for use by an extremist group. Particularly when it comes to biological agents, this threat will only become worse in coming years. We may soon, in fact, be faced not only with threats from known, naturally occurring pathogens but from genetically engineered ones as well.

In short, while the impact of terrorism to date has been horrific it is likely that this impact will increase dramatically in the future and that we will be feeling it for many years to come. We do not have the luxury of continuing to treat this issue as something that can be resolved by the application of standard bureaucratic measures. New lines on wiring diagrams and ever larger staffs will not win this conflict. Small numbers of highly trained, disciplined and creative individuals empowered to take risks and push the envelope will.

None of this is code for an acceptance of some of the more questionable practices of the Bush Administration. I am a staunch opponent of the so-called “enhanced” techniques used in questioning of al-Qaeda detainees. I have interrogated a large number of terrorist captives. None of them was ever harmed in any fashion. They all talked.

This is an argument that we need to accept, that we are--whether we like it or not--in a struggle with a very brutal, fanatical foe. This foe is not Islam. It is a group of fanatics who seek to drag that great faith and the entire Islamic world back into a dark, fantasy version of the Seventh Century. If anything, on some level, it is a war for Islam to preserve it from those who would hijack it and destroy it.

We would like to hope that we could find a way to combat this menace in some clean, anti-septic fashion. We would prefer that we could throw money at the problem, create a few new agencies and promulgate some regulations and that it would all be better. It will not, and the cost of not coming to grips with the problem will only increase. Someday, in the

near future, when a nuclear weapon goes off in New Jersey or the bubonic plague sweeps London, it may become unbearable.

Human intelligence (HUMINT) is, of course, only one facet of the intelligence world. That said, it always has been and always will be the only form of intelligence which will definitively tell you the enemy's intentions. Signals intelligence and imagery may alert you to the fact that the Russians are massing troops on their border with Georgia. Only HUMINT will tell you what was discussed in yesterday's late-night meeting in the Kremlin and whether the deployment is intended to make a political point or is, in fact, a precursor to invasion.

The impact of HUMINT is all that much greater in regard to terrorism and the emerging threats associated with it. A small al-Qaeda cell operating with discipline and exercising good tradecraft will leave almost no traces detectable by other means. They will deal in cash. They will stay off the phones. Their logistical requirements will be minimal. In short, absent source reporting, there will be little if anything for you to see via other intelligence means.

Even a cell working on a WMD attack will produce a profile far below that which many people expect. Biological weapons can be made and biological agents mass produced in a small apartment using commonly available materials. There are no technologies for remotely detecting such operations. You may well be able to use technical means to confirm what was being developed once you raid the apartment, but only after someone has told you where it is and alerted you to its significance.

In short, as noted above, there is no magic, antiseptic solution to problem with which we are faced. We need better human intelligence. Despite their obvious value, other forms of intelligence will not compensate for our failure to collect it. We have suffered grievous losses already as the consequence of our failure to address this issue. The losses we suffer in the future may make what has gone before seem inconsequential.

We need to undertake real intelligence reform, not changes calculated to satisfy bureaucrats and staff aides, but changes which produce real, tangible results. We need to fashion human intelligence collection mechanisms which can go out into the dark places of the world and bring back the critical information we need to defeat terrorist organizations and prevent attacks.

It is all well and good to talk about connecting dots, but we need to remember a simple truth: You cannot connect the dots until you first collect them.

Charles S. Faddis is currently President of Orion Strategic Services, LLC and is a former CIA Operations Officer and a former Head of the CIA's terrorist Weapons of Mass Destruction unit.