Statement for the Record

Lessons Learned and Actions Taken in Past Events

8 October 2002

Kie C. Fallis

Introduction

Chairman Graham, Chairman Goss and Members of these Committees: Thank you for the opportunity to address the issue of lessons learned and actions taken in past events. My comments of this subject will be addressed from the perspective of a counterterrorism analyst formerly assigned to the Defense Intelligence Agency. The many dedicated analysts in the Intelligence Community are the lynchpin of our nation's ability to successfully predict future events and to warn policy makers of important developments in the world. Successful intelligence analysis by itself is not extraordinarily difficult nor does it push any intellectual boundaries. It is a learned and trained process augmented by a background in a given field, and then developed through analytical software tools, databases and collaborative human minds. To accomplish this, an analyst must read and be familiar with as much information about their target as possible and to then communicate that knowledge in an effective and timely manner to their customers. When the situation warrants it, they will contribute to a formal warning process. As a subject matter expert in a given field, the analyst is also that person primarily responsible for identifying gaps in information and properly tasking the intelligence collection systems to gather the needed data. If the analysts fail to do their job, fail to read the collected intelligence, or fail to follow up on obvious intelligence gaps, the entire intelligence cycle will grind to a halt. The chances that we will be able to predict or prevent the next major act of terrorism are reduced to little more than dumb luck. However, with the proper tools, training and mandated sharing of intelligence information with properly cleared personnel, we will do better.

Terrorism Analysis as a Unique Field

There are significant differences in methodology between an all-source analyst studying a terrorist group and other all-source analysts in the Intelligence Community. These differences can potentially complicate accurate assessments and warnings, but are frequently not recognized even inside the counterterrorism community itself. While these differences need to be taken into account when examining past successes or

failures, they do not necessarily make the terrorism analyst's job any more difficult than their counterpart's.

The first, and arguably most important, distinction is the bureaucratic level at which meaningful advisories and warnings are communicated to intelligence consumers and to policy makers. In the case of a political/military all-source analyst, the closer the collector and/or analyst is to the subject the more likely they will be able to provide tactical warning of an upcoming event. For example, forward-deployed military intelligence units currently in Afghanistan will probably develop the critical details of an upcoming conventional attack against US interests, the who, what, where and when, before CONUS based analysts. This is due to their being physically on the ground with established liaison relationships, and by being able to exploit in-theater collection assets. Although this is a generalization and there have been several exceptions, most in the Intelligence Community do not expect DC-based analysts to provide specific tactical warnings of conventional attack to deployed units or to our Embassies abroad. They instead expect, and receive, strategic level assessments of recent activity and broad predictions of future actions. In the area of terrorism analysis, this recognized hierarchy is turned upside down. As this committee has already seen, a great deal of pertinent intelligence on terrorists and terrorist groups is collected, maintained and not adequately shared by, or even among, the major intelligence agencies. The more accurate and timely information is frequently retained by these agencies and not passed down the chain. When it is passed, the information is often watered-down or generalized in an attempt to protect sources and methods, as well as the need-to-know principle. There are numerous examples of this happening in the past and I will briefly discuss a few of them in another section. Consequently, our men and women assigned abroad for the State Department and the military are usually capable only of noting the broad details of a terrorist group's activities and are therefore more likely to be able to discern only strategic indicators of an upcoming attack.

The second notable difference between terrorism analysts and their all-source counterparts concerns the type of information available for incorporation into assessments and other intelligence products. Many all-source analysts are directed at subjects such as a nation-state, or some aspect of that target's capabilities where the

existence, location, leadership, etc is not hidden or in dispute. When examining these types of subjects, the potential sources of accurate information cover a wide spectrum from academic and press reporting to highly sensitive intelligence information. This is not usually the case with terrorism analysis. Since almost all terrorist groups, and certainly their operational cells, function in a closed, clandestine manner potential sources of accurate information are almost always limited to sensitive intelligence reporting. As a result, the terrorism analyst must work harder over a longer period of time in an effort to corroborate reporting and build an accurate profile of a group.

The third difference also concerns collected information, but is focused on the method by which the two types of analysts assess its veracity. Most all-source analysts take advantage of their wider spectrum of information in order to more easily verify its truthfulness. This variety also decreases the amount of experience and area knowledge needed by the analyst to correctly weigh the reporting. As noted above, the terrorism analyst is constrained, not by the volume of reporting, but usually by the number and types of sources. This lack of variety can cause problems when trying to verify current reporting in a timely manner and has a potentially negative impact on the warning process.

Terrorism Analytical Issues Complicating Improved Future Performance

The single most important issue that will affect future performance is the experience level of the analyst. While this certainly applies to all intelligence analysts regardless of subject area, it is even more critical for those trying to prevent the next terrorist attack. In the case of an analyst responsible for tracking a Middle Eastern terrorist group, this person will need to have an expertise, or at least a good working knowledge, of terrorism itself and the group, regional and country issues present in the group's operating area and Islamic history, culture and sects. As of October 2000, the Middle Eastern terrorism analyst who could claim that level of knowledge was by far the exception. For example, most new civilian hires and assigned military officers to DIA's Office for Counterterrorism Analysis lacked expertise in even one of these fields, much less all three. This was certainly not the fault of the DIA which was actually ahead of the

Community in attempting to hire additional analysts. The required levels of experience are almost never found in the civilian/academic world and are instead developed over time by training programs and in-house mentors.

Lack of experience has another impact on the terrorism analysis effort; namely the inability to consider current intelligence reporting in its proper historic perspective. In the period leading up to both the 1998 East Africa Embassy Bombings and the 2000 attack against the USS Cole in Yemen, terrorism analysts incorrectly assessed that a group would not conduct an attack in an area where it was able to operate with relative ease. Additionally, there appears to be a continued reluctance to correctly assess and evaluate the nature of cooperation between many Sunni and Shi'a Islamic extremist groups. Both of these examples, and there are certainly others, occurred despite over a decade of credible reporting to the contrary.

As the amount of information collected against al Qaeda and other terrorist groups continues to increase, each and every terrorism analyst must be given the tools to properly database that information. These tools do not necessarily need to be uniform, and the way an individual analyst uses the tools to improve his or her results will probably also vary by agency and mission. However, they must be used. The fragmentary and periodic nature of intelligence reporting on terrorism targets spans several years and cannot simply reside in an analyst's short-term memory. The frequent use of ever-changing actors, aliases and codewords is another unique challenge and significantly increases the chance of confusion and incorrect assessments. Only by carefully evaluating the veracity of collected information, properly noting its historic context (recent or otherwise) and then cataloguing it in a database tool will a terrorism analyst have any chance of connecting all the dots. Databases that also have the means to graphically represent their data will simplify and improve collaborative efforts with other intelligence analysts.

The other significant issue complicating future analytical performance against terrorists is the tendency of the FBI to compartment all pre- and post-attack investigative information. I realize this committee has spent a great deal of its time looking at the many legal and other aspects of this problem and I am not qualified to comment on those findings. However, as a former terrorism analyst and liaison officer to the FBI I can tell

you that having this information is critically important to being able to predict a future event. If the Community's analysts are left in the dark about how a group puts an attack together, and each group tends to do things a little differently, how will those analysts be able to pick up on future indicators? The investigative results of the 1996 Khobar Towers bombing were not disseminated until almost two years after the event and then only to a few select analysts and agencies. As a result, many analysts have incorrectly assessed al Qaeda as being culpable in this attack. These incorrect assessments in turn influence other products. Furthermore, since some of the individuals connected to this attack remain active in terrorism reporting, if an analyst is unaware of that person's role in a previous attack he or she will probably fail to attach the proper level of importance to that person's current activities. In another unfortunate example, US agencies conducted a vigorous investigation, to include a physical search, of the al Qaeda cell leader in Nairobi nearly a year prior to the 1998 Embassy bombings. Almost all of the results of this effort were never shared with the terrorism analytical community due to concerns about the criminal case. Most of the information was never properly exploited. In fact, a great deal of it was only translated after the bombings themselves. After the Embassy bombings, the post attack investigative results were again not shared. By failing to share this information, Bin Laden analysts were unable to build a correct modus operandi for al Qaeda attacks, and like the Khobar Towers example, they were unable to attach the proper level of importance to those culpable individuals still at large. This directly contributed to most analysts having only a moderate level of interest in the January 2000 Malaysia meeting of al Qaeda operatives, when in fact the same node that had organized a great deal of the East Africa Bombings was again active in organizing the Malaysia meeting.

Terrorism Warning Issues Complicating Improved Future Performance

The US has a well-developed and carefully thought out interagency terrorism advisory and warning system available to intelligence consumers and policy makers. The membership of various agencies, as well as the policy and procedures for issuing reports are carefully laid out and easily understood. In DOD's case, this interagency system is

augmented by its own which it can use separately or in conjunction with the other. Of note, DOD units at every level retain the authority to issue warnings if necessary. The ability of the US counterterrorism community to accurately predict and/or prevent the next terrorist attack against US interests should be priority number one and should be reflected in the quality of the warning products it issues. Unfortunately, inconsistent and vague advisories/warnings appear to have slowly diluted the system's effectiveness. Frequently, advisories have been issued not based upon the development of credible threat information, but rather upon the size or importance of an upcoming meeting, such as a gathering of major world leaders or a large sporting event. There are also inconsistent thresholds for issuing warning products among the major agencies. Some organizations appear willing to postpone an advisory until more complete information is received, while others will issue a warning based upon a single poorly-sourced intelligence report. These inconsistent thresholds are also usually apparent to the intelligence customer. In addition, there has been an inexplicable tendency on the part of some intelligence agencies to issue warning reports and raise the terrorism threat level after an attack.

As I noted earlier, most intelligence relating to terrorist groups is vague and fragmentary with the complete picture of a potential attack only developing after a period of several months, or even years. The fact that this information is vague should not deter warning officers, because when examined together the totality of the reporting usually results in a more complete and corroborated threat scenario. This is precisely what happened in the months leading up to the USS Cole attack. Almost all of the information required to predict or prevent this attack existed in intelligence databases, but since that puzzle had been in the process of being put together for almost a year, warning officers failed to appreciate the gravity of the last few reports on this subject since those reports did not appear to be out of the ordinary. This step-by-step approach to threat warning is the only realistic method available to us. The chance that our intelligence collectors, as good as they are, will stumble upon the who, what, where, when and how of a terrorist attack and then publish it in one or two messages is highly unlikely. Waiting for such a message is foolhardy.

Conclusion

The collection of additional information, further reorganizations and the hiring of additional analysts is unlikely to significantly affect any of these issues. The central hub in our nation's past, present and future failures or successes in the counterterrorism arena will rest squarely on the shoulders of the working-level analysts in both the law enforcement and intelligence communities. These men and women are the hard-working patriots who will have to try and find that single piece of hay in a stack of needles, and then try to tie it to another disparate piece of information in a timely manner. This will never be an easy job for them to accomplish, but the leadership of America's intelligence and law enforcement communities must provide them with the training, tools and information to accomplish the mission. The information they need to successfully predict and prevent the next terror attack is probably already contained in one or more community databases. The only question is whether experienced, working-level analysts will be given access to that information and will properly integrate that material into an accurate advisory or warning.