Senate Homeland Security and Governmental Affairs Committee

20 January 2010

Intelligence Reform: The Lessons and Implications of the Christmas Day Attack

Statement for the Record

of

Dennis C. Blair

Director of National Intelligence

Michael E. Leiter

Director of the National Counterterrorism Center

Statement for the Record

20 January 2010

Senate Committee on Homeland Security and Governmental Affairs
"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"

Chairman Lieberman, Ranking Member Collins, and Members of the Senate Committee on Homeland Security and Governmental Affairs: Thank you for your invitation to appear before the committee to discuss the counterterrorism efforts of the Intelligence Community and the improvements underway to fix deficiencies.

It is my privilege to be accompanied by Janet Napolitano, Secretary of Homeland Security, and Michael Leiter, Director of the National Counterterrorism Center.

The attempted terrorist attack on Christmas day did not succeed, but, as one of several recent attacks against the United States inspired by jihadist ideology or directed by al Qa'ida and its affiliates, it reminds us that our mission to protect Americans is unending.

Let's start with this clear assertion: Umar Farouk Abdulmutallab should not have stepped on that plane. The counterterrorism system failed and I told the President we are determined to do better.

Within the Intelligence Community we had strategic intelligence that al Qa'ida in the Arabian Peninsula (AQAP) had the intention of taking action against the United States prior to the failed attack on December 25th, but, we did not direct more resources against AQAP, nor insist that the watchlisting criteria be adjusted prior to the event. In addition, the Intelligence Community analysts who were working hard on immediate threats to Americans in Yemen did not understand the fragments of intelligence on what turned out later to be Mr. Abdulmutallab, so they did not push him onto the terrorist watchlist.

We are taking a fresh and penetrating look at strengthening both human and technical performance and do what we have to do in all areas. I have specifically been tasked by the President to oversee and manage work in four areas:

Immediately reaffirm and clarify roles and responsibilities of the counterterrorism analytic components of the IC in synchronizing, correlating, and analyzing all sources of intelligence related to terrorism.

Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence.

Take further steps to enhance the rigor and raise the standard of tradecraft of intelligence analysis, especially analysis designed to uncover and prevent terrorist plots.

Ensure resources are properly aligned with issues highlighted in strategic warning analysis.

NCTC has been tasked by the President to do the following:

Establish and resource appropriately a process to prioritize and to pursue thoroughly and exhaustively terrorism threat threads, to include the identification of appropriate follow-up action by the intelligence, law enforcement, and homeland security communities.

Establish a dedicated capability responsible for enhancing record information on possible terrorist in the Terrorist Identities Datamart Environment for watchlisting purposes.

The Events Leading Up to the Christmas Day Attack

I will now briefly discuss some of the details of the bombing attempt and what we missed. As the President has said, this was not—like in 2001—a failure to collect or share intelligence; rather it was a failure to connect, integrate, and understand the intelligence we had.

Although NCTC and the Intelligence Community had long warned of the threat posed by al Qa'ida in the Arabian Peninsula—to include as Director Leiter did with this Committee just this past Fall—we did not correlate the specific information that would have been required to help keep Abdulmutallab off that Northwest Airlines flight.

More specifically, the Intelligence Community highlighted the growing threat to US and Western interests in the region posed by AQAP, whose precursor elements attacked our embassy in Sana'a in 2008. Our analysis focused on AQAP's plans to strike US targets in Yemen, but it also noted—increasingly in the Fall of 2009—the possibility of targeting the United States. We had analyzed the information that this group was working with an individual who we now know was the individual involved in the Christmas attack.

In addition, the Intelligence Community warned repeatedly of the type of explosive device used by Abdulmutallab and the ways in which it might prove a challenge to screening. Of course, at the Amsterdam airport, Abdulmutallab was subjected to the same screening as other passengers—he passed through a metal detector, which didn't detect the explosives that were sewn into his clothes.

As I have noted, despite our successes in identifying the overall themes that described the plot we failed to make the final connections—the "last tactical mile"—linking Abdulmutallab's identity to the plot. We had the information that came from his father that he was concerned about his son going to Yemen, coming under the influence of unknown religious extremists, and that he was not going to return home. We also had other streams of information coming from intelligence channels that provided pieces of the story. We had a partial name, an indication of a Nigerian, but there was nothing that brought it all together—nor did we do so in our analysis.

As a result, although Mr. Abdulmutallab was identified as a known or suspected terrorist and entered into the Terrorist Identities Datamart Environment (TIDE)—and this information was in turn widely available throughout the Intelligence Community—the derogatory information associated with him did not meet the existing policy standards—those first adopted in the summer of 2008 and ultimately promulgated in February 2009—for him to be "watchlisted," let alone placed on the No Fly List or Selectee lists.

Had all of the information the U.S. had available, fragmentary and otherwise, been linked together, his name would have undoubtedly been entered on the Terrorist Screening Database which is exported to the Department of State and the Department of Homeland Security. Whether he would have been placed on either the No Fly or Selectee list—again based on the existing standards—would have been determined by the strength of the analytic judgment. One of the clear lessons the U.S. Government has learned and which the Intelligence Community will support is the need to modify the standards for inclusion on such lists.

In hindsight, the intelligence we had can be assessed with a high degree of confidence to describe Mr. Abdulmutallab as a likely operative of AQAP. But without making excuses for what we did not do, I think it critical that we at least note the context in which this failure occurred: Each day NCTC receives literally thousands of pieces of intelligence information from around the world, reviews literally thousands of different names, and places more than 350 people a day on the watchlist—virtually all based on far more damning information than that associated with Mr. Abdulutallab prior to Christmas Day. Although we must and will do better, we must also recognize that not all of the pieces rise above the noise level.

Intelligence Community Reform

While the December 25 attempt exposed improvement needs and flaws in coordination, it also revalidated the importance of intelligence efforts underway. The Intelligence Reform and Terrorism Prevention Act of 2004 and the progress of the past five years will continue to guide our future improvements. Let me acknowledge up front the vision and tenacity of Chairman Lieberman, Senator Collins, and the Members of this Committee as you developed and passed the 2004 Intelligence Reform Act. We share the goals you laid out in that legislation. The shortcomings that have been identified as a result of the December 25 attempt should not obscure the progress the Intelligence Community has made in improved collection and analysis capabilities, in improved collaboration and in sharing information, both against al Qa'ida and against the many other threats to our national security.

The United States Intelligence Community must constantly strive for and exhibit three characteristics essential to our effectiveness. The IC must be integrated: a team making the whole greater than the sum of its parts. We must also be agile: an enterprise with an adaptive, diverse, continually learning, and mission-driven intelligence workforce that embraces innovation and takes initiative. Moreover, the IC must exemplify America's values: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people.

The Intelligence Community has made significant strides in addressing the underlying deficiencies exposed by the attacks of 9/11. But, we must constantly improve and adapt.

To confront constantly evolving threats, we have made many changes in the way we conduct intelligence, law enforcement, homeland security, diplomatic, and defense activities since 2001. A prime example of improved integration is the new level of cooperation among FBI, local law enforcement and U.S. intelligence agencies in the recent arrests of Najibullah Zazi and David Headley, Americans allegedly associated with foreign terrorist organizations who are charged with planning attacks in this country and overseas. In both cases, tips and leads were smoothly passed among those gathering information in this country and those gathering information overseas, including foreign intelligence services that provided information or responded to questions.

Like our armed forces and first responders, intelligence professionals are on the front lines in defense of this country. Their operations are already collaborative between and across agencies to an extent that was unheard of five years ago. Continued commitment and investment in this reform are vital. If we become complacent now, or pessimistic about future progress, and revert to stovepipes and turf battles, full transformation will never be achieved.

In the area of information sharing, let me address areas where we have made progress and are focusing our future efforts:

Policy: The Office of the Director of National Intelligence (ODNI) has continued the transformation of information sharing by implementing Intelligence Community Directive (ICD) 501, "Discovery and Dissemination or Retrieval of Information." This ICD mandates wide-ranging actions to enable information sharing, including the ability to discover and request information from all IC elements, who now have a "responsibility to provide" such information. Implementation of the Intelligence Information Sharing Dispute Resolution process, formulated to simplify and streamline information sharing, has also produced positive results.

The Information Sharing Environment (ISE). The ISE is comprised of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of Federal, State, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration. In collaboration with our homeland security partners, fusion centers are able to access needed intelligence information for their mission, and in situations of information sharing conflict, procedures are in place to resolve information sharing issues.

Library of National Intelligence (LNI). The ODNI has made considerable progress on improving information sharing of finished intelligence across the IC through the creation of the LNI. The LNI is part of the DNI's efforts to build a more collaborative IC, improve information sharing, transform analysis, and modernize the IC's business practices. Access to LNI significantly improves access to critical expertise and the use of advanced tools to develop coordinated intelligence products.

Collaborative Tools/Capabilities. The creation and implementation of Intellipedia – the IC's version of the user-annotated online encyclopedia Wikipedia, has fostered spontaneous, collaborative analytic efforts, and has enhanced information sharing across the IC on current and emerging issues. Development of additional collaboration tools such as A-Space continues to improve IC information sharing capabilities. The creation of integrated information technology solutions and information sharing applications including consolidated e-mail naming conventions and information capabilities such as iVideo and Intelink further improve information sharing.

We are forging an integrated Intelligence Community that spans the historical divide between foreign and domestic intelligence efforts. Far from being a buzz word, integration means ensuring that our various specialized intelligence missions operate as a single enterprise. An integrated and collaborative Community is a critical advance because no single agency has the capacity to evaluate all available information—lest we forget over one billion pieces of data are collected by America's intelligence agencies everyday.

The principal legacy of the Intelligence Reform Act was the establishment of the Office of the Director of National Intelligence with assigned responsibilities to serve as the chief intelligence advisor to the President and to head the IC to ensure closer coordination and integration. The DNI is afforded responsibility to determine the National Intelligence Program and significant authority over personnel policy. In a larger sense, the creation of the DNI allows one person to see across the wide American Intelligence Community, identify gaps, and promote a strategic, unified direction.

Working closely with the Department of Justice and the FBI, we supported the creation of the FBI's National Security Branch to integrate the FBI's counterterrorism, counterintelligence, WMD, and intelligence programs.

We established the National Counterterrorism Center (NCTC), the government's hub for all strategic level counterterrorism intelligence assessments, which draws on collected terrorist intelligence from agencies across the U.S. Government with access to more than 30 different networks carrying more than 80 unique data repositories to produce integrated analysis on terrorist plots against U.S. interests at home and abroad.

The results are tangible. NCTC produces a daily threat matrix and situation reports that are the Community standard for current intelligence awareness. In addition, NCTC hosts two video teleconferences daily to discuss the threat matrix and situation reports to ensure the intelligence agencies and organizations see all urgent counterterrorism information.

We also established the National Counterproliferation Center (NCPC), the mission manager for counterproliferation, which has developed integrated and creative strategies against some of the nation's highest priority targets, including "gap attacks" (focused strategies against longstanding intelligence gaps), "over the horizon" studies to address potential future counterproliferation threats, and specialized projects on priority issues such as the Counterterrorism-Counterproliferation Nexus.

The establishment of the Department of Homeland Security (DHS) and DHS's Office of Intelligence and Analysis has enhanced the sharing of information between federal, state, and local government agencies, and the private sector which in turn has enhanced our ability to detect, identify, understand, and assess terrorist threats to and vulnerabilities of the homeland to better protect our Nation's critical infrastructure, integrate our emergency response networks, and link local state and federal governments.

The Terrorist Screening Center was created to consolidate terrorist watch lists and provide around the clock operational support for federal and other government law enforcement personnel across the country.

The growth and maturation of the FBI-led Joint Terrorism Task Forces (JTTF) in major jurisdictions throughout the United States has substantially contributed to improved terrorism-related information sharing and operational capabilities at the state and municipal levels.

Through these and other efforts, the United States and its coalition partners have made significant strides in defending the homeland against al-Qa'ida, its affiliates, and others who threaten us. Collaboration and information sharing have helped limit the ability of al-Qa'ida and like-minded terrorist groups to operate. We have uncovered and eliminated numerous threats to our citizens and to our friends and allies. We have disrupted terrorist plots, arrested operatives, captured or killed senior leaders, and strengthened the capacity of the Nation to confront and defeat our adversaries.

The Intelligence Community is an adaptive, learning organization. We can and must outthink, outwork, and defeat the enemy's new ideas. Our Intelligence Community is now more collaborative than ever before, knows how to operate as a team, and can adjust to conditions on the ground. We can and will do better, but I cannot guarantee that we can stop all attacks indefinitely. The integrated Intelligence Community as directed in the Intelligence Reform Act is essential; the basic elements of the system are sound; but we must be more flexible and anticipatory.

Fulfilling the goals expressed in the Intelligence Reform and Terrorism Prevention Act, in which this Committee played such a key role, was the right thing for national security in 2004 and is even more critical in 2010; the threats we face demand an integrated intelligence enterprise.