

**Prepared Testimony of Deputy Secretary of Defense Paul Wolfowitz
For the Senate Select Committee on Intelligence and
the House Permanent Select Committee on Intelligence:
Joint Inquiry Hearing on Counterterrorist Center Customer Perspective
September 19, 2002**

Chairman Graham, Chairman Goss, and Members of these Committees: You have long provided our country strong leadership and bipartisan support, especially now as America wages its war against terrorism. You demonstrate an example that America's security concerns transcend party or politics. I appreciate the opportunity to discuss with you today some Defense Department perspectives on the very important role of intelligence. I will keep my comments brief, as I believe my primary purpose today is to respond to your particular questions.

Let me first say that our thoughts and prayers are with the families of the victims of last September's attacks, some of whom testified before members of Congress yesterday. Last week, on the anniversary of the Pentagon attack, I was privileged to take part in a ceremony honoring those men and women who have labored so diligently and tirelessly over the last year to rebuild the Pentagon. I told them that their rebuilding of this symbol of America honored all those who died in the war against terrorism—those who died at the Pentagon, in New York, in Pennsylvania, and those who have died and are fighting for us now on frontlines around the world in this war against terrorism. I was able to meet with some of the family members; and while they, too, rejoiced in the outward healing that has taken place at the Pentagon since that day, it was all too evident that there is a hole in their hearts and many others that will never heal, and we grieve with them in their loss. But, seeing these family members whose lives were so fundamentally changed one year ago, I think, served to renew the commitment of each person who works in the Pentagon—military and civilian—to carry out the Department's mission in this war we wage against terrorism.

Yesterday, before a different committee on Capitol Hill, Secretary Rumsfeld addressed a dimension of this war against terrorism, referring to valuable intelligence information we already possess. He referred to President Bush, who said last week at the UN: "We know that Saddam Hussein pursued weapons of mass murder even when inspectors were in his country. Are we to assume that he stopped when they left?" The Secretary concluded, "To the contrary, knowing what we know about Iraq's history, no conclusion is possible except that they have and are accelerating their WMD programs."

Secretary Rumsfeld went on to observe that there are many now who are asking hundreds of questions about what happened on September 11th—poring over thousands of pages of documents, and asking who knew what, when, and why they didn't prevent that tragedy. He concluded, "I suspect that, in retrospect, most of those investigating 9/11 would have supported preventive action to pre-empt that threat, if it had been possible to see it coming."

He went on to make the point that if one were to compare the scraps of information the government had before September 11th to the volumes we have today about Iraq's pursuit of

WMD, Saddam Hussein's history of aggression and hostility toward the United States, and factor in our country's demonstrated vulnerability after September 11th—the case the President made should be clear.

The Secretary then added, "we cannot go back in time to stop the September 11th attack. But we can take actions now to prevent some future threats." Of course, that is precisely why we are here today—to examine how we may all work together to prevent future threats to our nation.

From the beginning, President Bush emphasized that the United States would fight this war using every element of national power—from diplomatic and law enforcement to intelligence and military elements. Certainly, one of the most important elements of national power, one we rely on today to help us prevent future threats, is the U.S. intelligence community. As evidenced by this hearing, these Committees are well aware of the fundamental importance of intelligence to our national security efforts, and have long been dedicated to providing valuable bipartisan support for intelligence-related programs.

Four years ago, I was honored to serve on the Rumsfeld Commission, which was charged with reporting to Congress on its assessment of the ballistic missile threat to the United States. Of course, one of the underlying focuses of our study was intelligence, as a look at such a threat would have been incomplete without considering our intelligence situation. When the Commission released its report in 1998, its nine commissioners—an almost even mix of Democrats and Republicans, holding a wide range of views—unanimously concluded that "U.S. analyses, practices and policies that depend on expectations of extended warning of deployment be reviewed and, as appropriate, revised to reflect the reality of an environment in which there may be little or no warning." While this conclusion came out of an assessment geared toward the ballistic missile threat, it was understood by each commissioner that the conclusion was applicable to all intelligence-related issues.

This was an understanding, I think, shared by those with whom we presented our findings, since members of Congress subsequently requested an Intelligence Side Letter, which elaborated on the Commission's intelligence concerns and made recommendations for change. First, according to the Side Letter, it was evident to all commissioners that resources for intelligence had been cut too deeply and that the United States was entering a period in which the intelligence community was going to be seriously challenged to meet its foremost task—preventing surprise. Second, one of the primary weapons in the endless struggle against surprise is knowing what our enemies don't want us to know. U.S. intelligence capabilities needed to succeed in this task, the letter concluded, were not as robust as they needed to be. Third, when there is more ambiguity in the intelligence material, the system becomes more dependent on analytic resources to discern the potential for surprise. The letter highlighted that in methodological approach, analytic depth and presentation to users, the intelligence community was in a degraded situation.

Following these conclusions, Congress responded with a significant increase in funding for intelligence in the FY1999 budget. Despite the best efforts of this Committee, however, the increases were not sustained in Fiscal Years 2000 or 2001. At the time of the attacks last

September, the Department was preparing a significant increase for intelligence in the FY2003 budget. After the attacks, this figure was doubled to the present proposal.

Lessons Learned from September 11th and its Aftermath

Before I outline some of the lessons drawn from September 11th and its aftermath, I would like to share with you a quote from Thomas Schelling's foreword to Roberta Wohlstetter's superb book, Pearl Harbor:

"Surprise, when it happens to a government, is likely to be a complicated, diffuse bureaucratic thing. It includes neglect of responsibility, but also responsibility so poorly defined or so ambiguously delegated that action gets lost. It includes gaps in intelligence, but also intelligence that, like a string of pearls too precious to wear, is too sensitive to give to those who need it. It includes the alarm that fails to work, but also the alarm that has gone off so often it has been disconnected. It includes the unalert watchman, but also the one who knows he'll be chewed out by his superior if he gets higher authority out of bed. It includes the contingencies that occur to no one, but also those that everyone assumes somebody else is taking care of. It includes, in addition, the inability of individual human beings to rise to the occasion until they are sure it is the occasion, which is usually too late. (Unlike the movies, real life provides no musical background to tip us off to the climax.)...The danger is not that we shall read the signals and indicators with too little skill; the danger is in a poverty of expectations, a routine obsessions with a few dangers that may be familiar rather than likely."

The expectation of the familiar must not guide us as we move forward. Rather the unfamiliar and the unlikely must be our new guides. With this in mind, let me discuss briefly some lessons from September 11th.

First, for past 50 years, US intelligence has concentrated on defeating external, nation-state threats. It is now clear that we must apply the same level of effort to non-state actors and threats that emanate from within our borders

Second, when people threaten openly to kill Americans, we should take them very seriously. That is true of Usama bin Laden and it is true of the regime in Baghdad. We must not assume that our enemies share our views about what is rational and irrational.

Third, we should not underestimate the skill of our enemies or their determination to conceal their activities and deceive us. They understand how we collect intelligence, how we are organized, and how we analyze information. Just like them, our intelligence services must constantly adapt and innovate. Thus, we have aggressive efforts underway to find new ways to discern terrorist "signals" from the background "noise" of society, but we must also recognize that enemies will deliberately create "noise" in the system in order to conceal the real signals.

Fourth, we must adapt our intelligence system to the information age. Old stovepipes must be broken down. A culture of compartmentation needs to be reconsidered. In all that we do, we must emphasize speed of exchange and networking to push information out to people who need it, when they need it, wherever they are.

Fifth, while we must always work to improve our intelligence we should never allow ourselves to believe that we can rely exclusively upon intelligence for our security. We should expect surprises and have capabilities that do not depend on perfect intelligence to defend the nation. As Secretary Rumsfeld observed yesterday, "We have had numerous gaps of two, four, six or eight years between the time a country of concern first developed a WMD capability and the time we finally learned about it."

Intelligence Transformation

Just as we are transforming the U.S. military, efforts are also underway that will ultimately result in the transformation of our intelligence posture.

Capabilities. Our current sources and methods have depreciated badly over the last decade. Sorely needed investments were postponed. Our budgets have been substantially increased as we are playing catch-up. There is no question that we need to recapitalize and introduce new sources of intelligence and novel methods of collecting and analyzing information. But our intelligence sources and methods have also been devalued by a culture of leaks through the Executive and Legislative Branches of government and a number of well-known espionage cases. Leaks and espionage have provided our adversaries, over time, with a very good picture of what we know and how we know it. One well-known instance involves the unauthorized disclosure of information that led Usama bin Laden to stop using a satellite phone that the U.S. had been monitoring. Once that information was out, we never again heard from his satellite phone.

Culture and Doctrine. A culture of excessive compartmentation will hinder our ability to defeat new threats. We need to facilitate greater sharing of information and collaboration with and between intelligence agencies, including law enforcement agencies, and analysts and collectors. Indeed, law enforcement agencies need to see their mission as prevention as much as apprehension. In many cases, our best hope of avoiding surprise will come from recognizing an ominous pattern in a mosaic of information that is collaboratively built. At the same time, it is true that compartmentation is necessary to prevent compromises of sources and methods.

Global terrorism now forces domestic and foreign intelligence systems to link together in order to prevent the enemy from finding a hiding place in the seam between these disciplines. It means that the executive and legislative branches have to work together to redefine the relationships and rules.

We must also accelerate the speed with which information is passed to policymakers and operators. We cannot wait for critical intelligence to be processed, coordinated, edited and approved – we must accept the risks inherent in posting critical information before it is processed.

We need to rethink the intelligence coordination process, whereby information is put through an analytic "filter" before it is passed on to policymakers. We need a more transparent process, one that gets alternative analyses up on the table quickly for policymakers to grapple with. We should not make the mistake of assuming that good intelligence analysis must arrive at

definitive or agreed conclusions.

Finally, we need to avoid making the mistake of thinking that intelligence estimates reached by consensus should routinely trump those of a lone dissenting voice. They don't.

During World War II, the United States and Britain assembled their best minds to crack the German code. These codebreakers, assembled at a place in England called Bletchley Park, defied the odds, accomplishing their vital mission faster than anyone expected. In doing so, they hastened the demise of Nazi Germany and the end of the war. As we seek to defeat terrorists and their supporters, our intelligence culture must renew the sense of urgency in collecting and mining and analyzing intelligence that inspired the codebreakers of Bletchley Park.

Organization. We need to continue to update a Cold War intelligence structure to better address 21st century threats. We are already taking steps to get our DoD house in order, and have proposed the creation of an Undersecretary of Defense for Intelligence (USD(I)) to streamline and integrate disparate DoD intelligence activities. The USD(I) is intended to provide the Department with a single staff office to oversee the various intelligence programs, and will support the existing relationship between the DCI and DoD seniors and provide a focal point for securing timely and effective support for the DCI from the Defense intelligence establishment.

This change will permit us to accelerate a large number of actions that are already underway. As this Committee knows, many of them are very highly classified, but there are a number that I can mention here.

- Issuing new contingency planning guidance to ensure U.S. forces have up-to-date contingency and operational plans;
- Establishing a Joint Intelligence Task Force for Combating Terrorism (JITF-CT) at DIA to help enhance our terrorist threat warning and analysis capabilities and significantly enhance connectivity and sharing between DIA, the FBI, and the CIA;
- Standing up a capability (the Joint Counterintelligence Assessment Group), in collaboration with the FBI and DoJ, to better identify and track terrorists;
- Standing up force protection detachments (FPDs) in high threat in-transit areas;
- Supporting large increases in personnel and funding for DoD intelligence activities, to include HUMINT, SIGINT, and All-Source Analysis;
- Providing combat air patrol, security augmentation at airports, and support to U.S. Customs Service, Border Patrol, and Immigration and Naturalization Service along our borders and southern borders;
- Establishing a combatant command for homeland defense – U.S. Northern Command (NORTHCOM). NORTHCOM will focus on defending the people and territory of the U.S. against external threats and on coordinating the provision of U.S. military forces to support civil authorities.

We also need to address a relatively new problem, what I'll call "information discovery." Many agencies collect intelligence and lots of agencies analyze intelligence, but no one is responsible for the "bridge" between collection and analysis. Who in the intelligence community is responsible for tagging, cataloguing, indexing, storing, retrieving, and correlating data or for facilitating collaboration involving many different agencies? Given the volume of information that we must sift through to separate signal from noise, this function is now critical. We cannot neglect it.

There is much more that we can do to exploit the full benefits of new information technologies such as data mining and change detection, as well as the steadily decreasing cost of data storage. Partly because of the inescapable need for security of information, the intelligence community lags behind the private sector in its ability to tag and store massive amounts of data, and to mine that information to determine patterns. Again, a culture that discourages collaboration and the sharing of information forfeits these new technological advantages.

One more issue we must consider is how we consider "need to know." We need to break down the access to information so that those who need it, get access to it. It is interesting to recall that, before Pearl Harbor, an ultra-secret code-breaking operation, one of the most remarkable achievements in American intelligence history, an operation called "Magic," had unlocked the most private Japanese communications, but the operation was considered so secret and so vulnerable to compromise that the distribution of its product was restricted to the point that our field commanders didn't make the "need to know" list. But, it is easy to say in hindsight that this information should have been shared more widely. If it had been, and had been compromised as a result, we would have been asking ourselves why it was shared too widely.

Conclusion

In closing, I would emphasize three points. First, as I mentioned, the President has said that the United States would fight this war using every element of national power—from diplomatic and law enforcement to intelligence and military elements, with America's military power not necessarily the first option, but one of a vast array of national resources with which to fight. Certainly one of the most important elements in fighting this war of the shadows involves the U.S. intelligence community and its extraordinary capabilities. Whatever is done to reform or improve the intelligence community should do no harm to our current war effort.

Second, no matter how good intelligence gets to be, we will not win this war simply by going after individual terrorists. We must not only capture and kill terrorists, but we must drain the swamp in which they breed.

In February, 1998, Usama bin Laden published a "fatwa" declaring his intent to kill Americans, a fact that leads to my third conclusion: when our professed enemies declare that they intend to kill us, we must take them at their word, and prepare accordingly. We must avoid the temptation of believing the truth can only be found through classified sources. To do otherwise, despite warnings and signs, would indeed constitute a grave intelligence failure.

Secretary Rumsfeld testified yesterday to some of the signs and signals that now abound, saying that we are on notice. "Let there be no doubt, he said, "an attack will be attempted. The only question is when and by what technique. It could be months, a year, or several years. But it will happen.... If the worst were to happen, not one of us here today will be able to honestly say it was a surprise. Because it will not be a surprise," he said. "We have connected the dots as much as it is humanly possible—before the fact. Only by waiting until after the event could we have proof positive. The dots are there for all to see. The dots are there for all to connect. If they aren't good enough, rest assured they will only be good enough after another disaster—a disaster of still greater proportions. And by then it will be too late."

The President has made clear we will not wait until it is too late and that the one option we don't have is to do nothing. We cannot afford to wait, as the Secretary put it so well, "until we have a smoking gun. For a gun smokes after it's been fired."

We appreciate this Committee's dedication to accomplish meaningful, positive and constructive measures with regard to America's intelligence community. We appreciate your continued bipartisan leadership and guidance. And we look forward to working with you in your fundamentally important task of looking to the future as we improve America's intelligence capability.