S. HRG. 107–224

DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MARCH 27, 2001

Serial No. J–107–8

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
76–917 DTP WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina	PATRICK J. LEAHY, Vermont
CHARLES E. GRASSLEY, Iowa	EDWARD M. KENNEDY, Massachusetts
ARLEN SPECTER, Pennsylvania	JOSEPH R. BIDEN, JR., Delaware
JON KYL, Arizona	HERBERT KOHL, Wisconsin
MIKE DEWINE, Ohio	DIANNE FEINSTEIN, California
JEFF SESSIONS, Alabama	RUSSELL D. FEINGOLD, Wisconsin
SAM BROWNBACK, Kansas	CHARLES E. SCHUMER, New York
MITCH MCCONNELL, Kentucky	RICHARD J. DURBIN, Illinois
	MARIA CANTWELL, Washington

SHARON PROST, *Chief Counsel*
MAKAN DELRAHIM, *Staff Director*
BRUCE COHEN, *Minority Chief Counsel and Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

JON KYL, Arizona, *Chairman*

MIKE DEWINE, Ohio	DIANNE FEINSTEIN, California
JEFF SESSIONS, Alabama	JOSEPH R. BIDEN, JR., Delaware
MITCH MCCONNELL, Kentucky	HERBERT KOHL, Wisconsin
	MARIA CANTWELL, Washington

STEPHEN HIGGINS, *Majority Chief Counsel*
DAVID HANTMAN, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION

TUESDAY, MARCH 27, 2001

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:10 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl, Chairman of the Subcommittee, presiding.

Present: Senators Kyl and Feinstein.

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Chairman KYL. The Subcommittee will come to order. I welcome everyone to this hearing of the Subcommittee of the Judiciary Committee on Technology, Terrorism, and Government Information.

By way of apology, let me first say that we had three votes which delayed the party luncheons, as a result of which some of the Senators will be late. I am informed that Senator Feinstein has an additional meeting, and therefore she may be quite a little bit late. But with that information, I am going to go ahead because I don't want to keep all of you waiting.

At this hearing today, we are going to examine the findings of the Congressionally mandated Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, as presented in its latest report entitled "Toward a National Strategy for Combating Terrorism."

At the dawn of this new millennium, the United States faces new challenges to the security of our Nation, our people, and interests abroad. We face no peer rival, and our view of the horizon is no longer clouded by the once ominous threat of either a large-scale nuclear attack on our homeland or a massive conventional attack on our European allies.

Yet, the security our citizens both at home and abroad is threatened. The threat no longer derives from a single source, but from a myriad of sources, including terrorists organizations that increasingly see Americans and their interests as their premier targets.

The means available to terrorist organizations and their sponsors are potentially more deadly and catastrophic than ever. We have only to look back to October of last year and the devastation

wrought by two men in a small boat heavily laden with conventional explosives that maneuvered alongside the USS Cole. Seventeen American sailors perished, with many others wounded, and an American war ship was reduced to a crippled hulk in just a matter of a few seconds.

In the 1990's, 6 people were killed and 1,000 were injured in bombing of the World Trade Center in New York City. But the bombers' goal was to topple the twin towers, which would probably have killed tens of thousands of people. Imagine the destruction if those responsible for these attacks had been more technically proficient or if they had had weapons of mass destruction.

The perpetrators of these attacks do not appear to be state-sponsored organizations in the classic sense. Recent reports have strengthened the links between the Cole bombing and exiled Saudi millionaire Usama Bin Ladin. Although not state-sponsored in the classic sense, Bin Ladin is dependent upon a variety of states for asylum and protection of his assets. The fact that his group is not state-sponsored does not mean it is less threatening.

According to the Director of the National Security Agency, Bin Ladin can afford to outfit himself with better and more sophisticated communications equipment than most of the agencies of the U.S. Government that might be charged with countering his efforts.

According to recent foreign press reports, Bin Ladin's financial empire has enabled his supporters to strengthen their hold upon the Taliban government of Afghanistan, thereby eliminating the likelihood of extradition. If Bin Ladin can afford all of this, someday he may even be able to buy a nuclear, chemical, or biological weapon and the means to employ it.

The emergence of terrorist groups that are not state-sponsored does not mean that nations no longer support terrorism. For example, Iran continues to be the most active state sponsor of terrorism. Tehran already has chemical and biological weapons. In fact, nearly all of the seven nations that the U.S. identifies as state sponsors of terrorism are believed to possess weapons of mass destruction of at least some capability.

Given this state of affairs, what should U.S. strategy be and how can we effect it? The Panel to Assess Domestic Response Against Terrorism was quick to realize that the presence of the word "Domestic" in its name did not limit it to the study of strictly domestic solutions to strictly domestic weaknesses.

The members, representing a broad cross-section of local, State and Federal expertise, came to the conclusion that much of the deterrence and prevention of terrorism must begin on foreign soil, with strong partnerships among our allies and an equally strong intelligence capability.

The panel made several recommendations aimed at strengthening our ability to both gather intelligence on terrorist organizations and share intelligence between agencies responsible for countering the terrorist threat. The panel also made numerous recommendations designed to improve the cooperation between Federal, State and local entities to enhance our capability to respond to a catastrophic terrorist attack.

In our first of two panels today, we are pleased to be joined by Vice Chairman of the Advisory Panel, Lieutenant General James Clapper, who formerly served as Director of the Defense Intelligence Agency. The Chairman of the Advisory Panel, Governor James Gilmore of Virginia, was invited to attend, but could not be here due to a scheduling conflict.

I might say that we decided to proceed with this hearing because it is our intention, both Senator Feinstein and myself, to take as much testimony as we can within a period of just a few weeks and begin to put together legislation that we can actually have an opportunity to run this year with an expectation that we could get it passed. We believe that if we take the best of the suggestions from this panel and from other panels that have addressed the same general subject matter and put them together into a package, we can perhaps begin to coordinate the efforts much better than they are and at least add the legislative perspective to it that we think may be required.

The second panel today includes two of our Nation's foremost experts on terrorism and national security. Dr. Anthony Cordesman currently serves as the Distinguished Arleigh Burke Chair and Senior Fellow at the Center for Strategic and International Studies. He has overseen and participated in a series of studies on terrorism and asymmetric warfare, and has a long history as an analyst of national security issues.

Dr. Yonah Alexander is a Senior Fellow at the Potomac Institute and Director of its International Center for Terrorism Studies. He is the founder and editor of "Terrorism," an international journal.

I will afford Senator Feinstein the opportunity, if she arrives, to fit her statement in wherever we are in the testimony, and any member of the Subcommittee will have an opportunity to submit their statements for the record.

[The prepared statement of Senator Sessions follows:]

STATEMENT OF HON. JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA

I am very glad that Senators Kyl and Feinstein called this hearing today. This country faces a real threat. I am afraid that the question about whether a chemical, biological, radiological, nuclear, or cyber-terrorist attack will happen in the United States is less a question of whether, than of when. As the anniversary of the most heinous attack in America history—the Oklahoma City bombing on April 19, 1995—draws near, we remember what terrorism can do to this country. Not only were lives lost in that attack, but fear was allowed to rule us. That bomb was very simply constructed—just a bunch of diesel fuel and fertilizer in a moving van—yet it ripped a building in half, killing 168 people and wounding many others.

Now, imagine a terrorist walking into an airport or football stadium or even, God forbid, this building, with a nerve agent like VX. With an amount less than a drop of water, that terrorist has a weapon to kill even more people than in Oklahoma City. That would be harder to detect and even harder to prevent or contain once an attack occurred.

Worse yet, imagine a coordinated attack from all fronts. First, a computer terrorist sabotages U.S. government and military computers, shutting down lines of communication and defense. At the same time, he strikes civil telecommunications and financial services. Topping all that with a traditional military deployment by a rogue state, America would have a tremendous and frightening challenge to overcome.

Luckily, this country is already on the ball. Many agencies such as the Department of Defense, the Department of State, the Department of the Treasury, the Department of Justice, the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation, the Public Health Service component, and the Department of Energy have all taken substantial steps, along with over 50 other organiza-

tions throughout the U.S. Government, to make sure that a domestic terrorist attack does not occur, and if it does, that we have the best ways to deal with it. Four different reports, issued by four different groups looking specially at this problem, have assessed the threat of domestic terrorism and come up with ideas on how to address that threat. Today's distinguished panel of witnesses will give us more insight into one of these reports—the second in a series of RAND reports issued by the Gilmore Commission.

I agree with all four reports that there is a huge need for greater coordination between the responsible agencies and between the federal, state, and local entities responsible for detecting, stopping, and responding to an attack in their particular community. Each of these reports presents a possible but slightly different solution to the problem. However, I think we need to really look hard at whether one of the four solutions will work best or whether we need a combination of all four.

I also agree with my colleagues here today, Senators Kyl and Feinstein, who last session introduced solid legislation aimed at finding counter terrorism strategies and solutions. This legislation passed the Senate. The bill takes an important first step towards solution to this problem.

First, it is important that we keep Syria and Iran on the Foreign Terrorist Organization list. There are indications that both countries continue to sponsor terrorist groups with ill will towards the United States.

Second, the reports and task forces required by this bill will ensure that we have answers to important questions: (1) how to improve the guidelines on recruiting terrorist informants to encourage them to spill the beans on their cohorts ; (2) where research and development may improve the technologies to combat terrorists on American soil; (3) how to get the best information disseminated to the agencies dealing with the problem; (4) what needs to be done to stop existing world-wide terrorist fund-raising efforts; and (5) how we can improve the monitoring of domestic sales and lab handling and storage of biological agents and the equipment needed to use them.

Senator Kyl's and Senator Feinstein's previous bill had the making of a crucial first step in the war on terrorists. Another fundamental step in domestic preparedness is the continual need to train first responders such as fire fighters, police officers, and emergency medical crews. Since we do not know where an attack using a weapon of mass destruction (WMD) will occur (it could be the Nation's Capital, another big urban center, or even in small town America) we need to be prepared across the Nation. To accomplish that preparedness means we need to train and equip our civilian responders to the highest standard possible.

Traditionally, the military has been responsible for dealing with attacks on the United States. However, the military is not and cannot be on hand in every community on a 24-hour basis. That's why first responders are so important.

In my home state of Alabama, we have the nation's only Center for Domestic Preparedness that trains with the actual chemical and biological substances that might be used in an attack. Exercises run in the Chemical Training Facility-identical to the training used by our military forces at Ft. Leonardwood, Missouri—is the only way to test how firefighters, policemen, and other first responders will react under pressure, taking away the fear of the unknown that is present whenever an invisible hand strikes. Incredibly, this Center -has already trained 5,000 first responders, but the nation needs to train many, many more. Politicians of every political persuasion have recognized the importance of this Center to the overall domestic preparedness picture. Our former Attorney General, Janet Reno, called the Center a "crown jewel" in testimony before Congressional Committees.

In conclusion, I want to again thank Senator Kyl and Senator Feinstein for holding this hearing and for developing legislation that is an important first step in dealing with the problems.

Chairman KYL. So with that, let me introduce our first witness, Lieutenant General Clapper, Vice Chairman of the Advisory Panel and former Director of the DIA.

General Clapper, welcome. Thank you for taking time to be here. We will place your full statement in the record and invite you to make whatever summary remarks you would like to make at this time.

STATEMENT OF LIEUTENANT GENERAL JAMES CLAPPER, JR., UNITED STATES AIR FORCE (RETIRED), VICE CHAIRMAN, ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION, WASHINGTON, D.C.

General CLAPPER. Thank you very much, Mr. Chairman. I am very pleased to have this opportunity to speak to you as Vice Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, less awkwardly known as the Gilmore Commission.

You have asked that we provide testimony today on the findings and recommendations in our second report, which is the second of three, and we go out of business at the end of this year. I will outline those recommendations and will discuss particularly two of them, one dealing with the need for a national strategy and the other the need for somebody to be in charge.

You have also asked that I speak to areas of agreement and disagreement between the Gilmore Commission and the National Commission on Terrorism, chaired by former Ambassador L. Paul Bremer, who I might mention is also a member of the Gilmore Commission. So we did have fortuitously good cross-over there.

With respect to strategy, it is our belief, our conviction, after looking at this for a couple of years now that there is, in fact, no overarching statement of what the United States is trying to achieve with its program to combat terrorism.

Instead of a national strategy, what we really have is a loosely coupled set of plans and programs that aim individually to achieve certain particular preparedness objectives. Senior U.S. officials have stated that several official broad policy and planning documents that were published during the prior administration, such as the Presidential Decision Directives 39 and 62, the Attorney General's 1999 Five-year Interagency Plan, and the most recent Annual Report to Congress on Combating Terrorism, taken as a whole constitute a national strategy.

Our view is that these documents describe plans, the compilation of various programs underway, and some objectives, but they do not either individually or collectively constitute a national strategy. As a result, we recommended that the incoming administration develop such a national strategy by laying out national goals for combating terrorism focusing on results—that is, outputs rather than process or inputs.

We made three key assumptions to guide the strategy development. The first assumption was that local response entities, meaning law enforcement, fire services, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers, will always be the first, and conceivably only response.

Second, in the event of a major terrorist attack, however that is defined, no single political jurisdiction is likely to be capable of responding to such an attack all by itself without some outside assistance.

Third, and perhaps most important, we already have existing emergency response and management capabilities, developed over many years, for response to natural disasters, disease outbreaks,

and accidents. Those capabilities should be used as a base for enhancing our domestic capability for response to terrorist attack.

I want to highlight some of the attributes of the national strategy that we outlined in our report. It should be geographically and functionally comprehensive. It should address both international and domestic terrorism. That distinction, heretofore somewhat nice, neat, separate compartments between domestic and foreign, is gradually eroding, we believe.

The national strategy should address the full spectrum of the Nation's efforts against terrorism, to include intelligence, deterrence, prevention, investigation, prosecution, preemption, crisis management, and consequence management. The national strategy should apply to the Nation as a whole, not just the Federal executive branch, and must involve States and communities as essential and equal partners.

With respect to the issue of placing someone in charge, it has been our observation based on a lot of discussion, briefings, and travel, that many at the State and local levels perceive the structure and processes at the Federal level for combating terrorism as uncoordinated, complex, and confusing.

Our first report included a graphic depiction of the numerous Federal agencies and offices within those agencies that have responsibilities for combating terrorism. I testified this morning before a House panel looking at this and they had extracted the graphics from our first report and had them displayed in the Committee room, which basically was one organizational chart after another of all the departments and agencies who in one way or another, one degree or another are involved in combating terrorism, a very effective graphic depiction.

Attempts to create a Federal focal point for coordination with State and local officials such as the National Domestic Preparedness Office have been only partially successful. Moreover, many State and local officials believe that Federal programs are often created without consulting them. And confusion often exists even within the Federal bureaucracy. It is our view that the current coordination structure does not possess the requisite authority or accountability to make policy changes and to impose the discipline necessary among the numerous Federal agencies involved.

So for those and other reasons, we have recommended the establishment of a senior-level coordination entity in the Executive Office of the President entitled the National Office for Combating Terrorism, with responsibility for developing domestic and international policy, and for coordinating the program and budget of the Federal Government's activities for combating terrorism.

The title of the entity is not as important as its responsibilities and authorities, and I should interject here since it came up this morning that we had great aversion to the term "czar," which is often applied perhaps to such a construct, and we would not choose to use that term.

The responsibilities and functions of this organization tethered to the President would be forging a national strategy, and this would be, I think, its first and foremost responsibility, managing the program and budget by a process of certifying or decertifying the

budgets of the other agencies and departments involved in combating terrorism.

A subject near and dear to my heart is fostering intelligence collection, analysis, and most importantly dissemination particularly and especially to State and local officials; reviewing plans of State and local authorities to ensure synchronicity or coordination with the national strategy; coordinating health and medical programs; directing research development, test, and evaluation, and developing national standards; and serving as sort of the one-stop shop, if you will, for information as a clearinghouse for State and local officials.

Two other attributes I want to mention are that we feel this entity or office should have political accountability and responsibility. The person designed as the focal point to be in charge for developing a national strategy and for coordinating Federal programs must have this political accountability and responsibility. Ergo, our recommendation was that this person should be appointed by the President and confirmed by the Senate, and would enjoy Cabinet-level rank.

At the same time, we also would emphasize that this organization would not have operational control over Federal agency activities. In other words, the execution would still remain with the various Government departments and agencies. It was not our intent in any way that those departments and agencies should abrogate their responsibilities. What we are advocating is more coherence, more coordination which would be brought about by this office for coordination of counterterrorism.

At the risk of perhaps going where angels fear to tread, I also wanted to mention the Congress in this. Its intention, I think, has been helpful, but in a sense the Congress has also contributed to the executive branch's problems.

Over the past 5 years, there have been half a dozen Congressional attempts to reorganize the executive branch's efforts to combat terrorism, all of which failed. None enjoyed the support of the executive branch. At least 11 full committees in the Senate and 14 full committees in the House, as well as their numerous subcommittees, claim to one degree or another some oversight responsibility for various aspects of programs for combating terrorism.

Earmarks in appropriations bills created many of the Federal Government's specific domestic preparedness programs without authorizing legislation or oversight. The huge appearing, at least, U.S. budget for combating terrorism is now laced with such earmarks which have proliferated in the absence of an executive branch strategy.

The executive branch cannot successfully coordinate its programs for combating terrorism alone. Congress, we think, must also better organize itself and exercise much greater discipline. So we have recommended creation of a joint committee, or alternatively separate committees in each House somewhat akin to the construct I am used to, the two intelligence oversight committees, to pass on executive branch requests and to oversee execution of programs that it authorizes.

Obviously, for this to work, other Congressional authorizing and appropriations committees would have to defer to the joint or the

single Committee in each House. We are not so naive to think this recommendation is any less difficult than the executive branch changes that we are proposing, but it is no less needed.

We also made six specific functional recommendations in the following areas, and I will simply tick off the subject matter areas rather than dwelling on them, since there is a detailed discourse on that in my prepared statement.

The functions we had in mind for this National office would be to foster the collection of intelligence, assessing threats and sharing information particularly at the State and local level; operational coordination, training, equipping, exercising, overseeing and facilitating health and medical coordination; research development and promulgation of national standards; and providing cyber security against terrorism.

You asked, sir, for a discussion of the areas of agreement and disagreement with the report of the National Commission on Terrorism which was chaired by Ambassador Jerry Bremer, who, as I said, is on our panel as well.

First, I would mention that the charters and objectives of the Bremer Commission and the Gilmore Commission are for the most part different. The Bremer Commission focused on international terrorism, while we focused on domestic preparedness.

There are, nevertheless, many congruent areas between the two reports. Both agree on the nature of the threat of international terrorism, including the potential for more attacks inside the borders of the United States. Both panels specifically agree that certain measures must be taken to improve intelligence collection and dissemination on terrorists, including repealing the 1995 Director of Central Intelligence guidelines as they apply to recruiting terrorist informants, reviewing and clarifying the Attorney General's guidelines on foreign intelligence collection and the guidelines on general crime racketeering enterprise and domestic security terrorism investigations, and directing the Department of Justice Office of Intelligence Policy and Review not to require a process for initiating actions under the Foreign Intelligence Surveillance Act that are more stringent than what was actually required by the statute.

Both panels agree that significant improvements must be made in the ability of intelligence and law enforcement agencies to collect, analyze, disseminate, and share information. Both panels agree that there must be a comprehensive strategy to deal with terrorism.

Both panels agree that the Department of Defense and U.S. armed forces may have a major role in preventing or responding to a terrorist attack, especially a major one. We likewise strongly agree that more planning, coordination, training, and exercises need to be conducted to prepare for the possibility of major DoD and military involvement.

The one area, however, on which the two panels disagreed had to do with the issue of lead agency. The Bremer Commission asserts that a response to a catastrophic attack may require the designation of DoD as lead agency. While agree that DoD may have, and probably would have a major role in such a cataclysmic event, we believe firmly that the military must always be directly under civilian control.

I can speak personally that Governor Gilmore feels personally very strongly about this. This was probably the most hotly debated and discussed issue in the 2 years of the existence of our panel. So as a result, we recommended that the President always designate a Federal civilian agency other than the Department of Defense as the lead Federal agency.

Many Americans will not draw the technical distinction between the Department of Defense, the civilian entity, and the U.S. armed forces, the military entity. Although the Department of Defense and every major component of the Department has civilian leaders, the perception will likely be that the military is in the lead. And in the interest of preserving our civil liberties, or even dispensing with the risk of jeopardizing civil liberties, it was our conviction after a lot of discussion and debate that the lead Federal agency in every case should be a genuine civilian element.

In conclusion, Mr. Chairman, Gilmore panel members are convinced that the recommendations that I have outlined here briefly are crucial to strengthening the national effort to combat terrorism. We need a true national strategy and we need somebody in charge. This is not a partisan political issue. We have members on our panel who identify with each of the parties, virtually all the functional constituencies, and at all governmental levels. This is simply something that we unanimously agreed that the country needs.

Contemplating the specter of terrorism in this country is a sobering but critically necessary responsibility of government officials at all levels and in all branches, as evidenced by your interest this afternoon. It is truly a national issue that requires synchronization of our efforts vertically among the Federal, State and local levels, and horizontally among the functional constituent stakeholders.

The individual capabilities of all critical elements must be brought to bear in a much more coherent way than is now the case. That fundamental tenet underlies our work over the last 2 years. We believe that the most imposing challenge centers on policy and whether we have the collective fortitude to forge change both in organization and process.

I would respectfully observe that we have studied the topic to death and what we need now is action.

Mr. Chairman, this concludes my statement. I would be pleased to address your questions.

[The prepared statement of General Clapper follows:]

STATEMENT OF JAMES CLAPPER, JR., LIEUTENANT GENERAL, U.S. AIR FORCE, RETIRED, VICE CHAIRMAN, ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION, WASHINGTON, D.C.

Mr. Chairman, Members of the Subcommittee, I am honored to be here today. I come before you as the Vice Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, also known as the "Gilmore Commission" (after its Chairman, Governor James S. Gilmore, III, of Virginia). Thank you for the opportunity to present the views of the Advisory Panel.

The Advisory Panel was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 10–261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998). That Act directed the Advisory Panel to accomplish several specific tasks. It said:

The panel shall——

1. assess Federal agency efforts to enhance domestic preparedness for incidents involving weapons of mass destruction;
2. assess the progress of Federal training programs for local emergency responses to incidents involving weapons of mass destruction;
3. assess deficiencies in programs for response to incidents involving weapons of mass destruction, including a review of unfunded communications, equipment, and planning requirements, and the needs of maritime regions;
4. recommend strategies for ensuring effective coordination with respect to Federal agency weapons of mass destruction response efforts, and for ensuring fully effective local response capabilities for weapons of mass destruction incidents; and
5. assess the appropriate roles of State and local government in funding effective local response capabilities.

The Act requires the Advisory Panel to report its findings, conclusions, and recommendations for improving Federal, State, and local domestic emergency preparedness to respond to incidents involving weapons of mass destruction to the President and the Congress at three times during the course of the Advisory Panel's deliberations-on December 15 in 1999, 2000, and 2001.

Mr. Chairman, you have asked that we provide testimony today on the findings and their related recommendations contained in the second report of the Advisory Panel, entitled "Toward a National Strategy for Combating Terrorism," dated December 15, 2000. I will outline those recommendations, and will provide a more detailed description on two of them-one dealing with the need for a national strategy, the other on the structure of the Executive Branch for dealing with terrorism. You have also asked that I note the areas of agreement and disagreement that the Gilmore Commission has with the report of the National Commission on Terrorism, which was chaired by former Ambassador L. Paul Bremer.

PRINCIPAL FINDINGS AND RECOMMENDATIONS IN THE SECOND ANNUAL REPORT

A NATIONAL STRATEGY FOR COMBATING TERRORISM

"The United States has no coherent, functional national strategy for combating terrorism; and the next President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office."

Mr. Chairman and Members, the Advisory Panel believes that a truly comprehensive national strategy will contain a high-level statement of national objectives coupled logically to a statement of the means to be used to achieve these objectives. Currently, there is no overarching statement of what the United States is trying to achieve with its program to combat terrorism. Goals must be expressed in terms of results, not process. Government officials have, in the past, spoken of terrorism preparedness goals in terms of program execution. A comprehensive national strategy will answer the more fundamental and important question: To what end are these programs being implemented?

Instead of a national strategy, the nation has had a loosely coupled set of plans and specific programs that aim, individually, to achieve certain particular preparedness objectives. Senior U.S. officials have previously stated that several official broad policy and planning documents that were published in the prior administration-Presidential Decision Directives 39 and 62, the Attorney General's 1999 Five-Year Interagency Counterterrorism and Technology Crime Plan, and the most recent Annual Report to Congress on Combating Terrorism [1]—taken as a whole, constitute a national strategy. These documents describe plans, the compilation of various programs already under way, and some objectives; but they do not either individually or collectively constitute a national strategy.

Although Executive Branch agencies are administering programs assigned to them in the various pieces of legislation, the Executive Branch, under the former administration, did not articulate a broad national strategy that would synchronize the existing programs or identify future program priorities needed to achieve national objectives for domestic preparedness for terrorism. Moreover, it is our view that, given the structure of our national government, only the Executive Branch can produce such a national strategy.

As a result, we recommended that the incoming Administration begin the process of developing a national strategy by a thoughtful articulation of national goals for combating terrorism, focusing on results rather than process. The structure and spe-

[1] The Office of Management and Budget, Annual Report to Congress on Combating Terrorism, Including Defense against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection, May 18, 2000.

cifics of the national program should derive logically and transparently from the goals, not the other way around.

BASIC ASSUMPTIONS

The Advisory Panel agreed on several basic assumptions to guide its approach to strategy development. First, "local" response entities-law enforcement, fire service, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers—will always be the "first" and conceivably only response.

Second, in the event of a major terrorist attack, however defined—number of fatalities or total casualties, the point at which local and State capabilities are overwhelmed, or some other measure—no single jurisdiction is likely to be capable of responding to such an attack without outside assistance. That assumption is critical to understanding the need for mutual aid agreements and coordinated operations.

Third—and perhaps most important—there are existing emergency response and management capabilities, developed over many years, for responses to natural disasters, disease outbreaks, and accidents. Those capabilities can and should be used as a base for enhancing our domestic capability for response to a terrorist attack. We can strengthen existing capabilities without buying duplicative, cost-prohibitive new capabilities exclusively dedicated to terrorism.

MAJOR ELEMENTS OF THE NATIONAL STRATEGY

The national strategy should be geographically and functionally comprehensive. It should address both international and domestic terrorism. The distinction between terrorism outside the borders of the United States and terrorist threats domestically is eroding. International terrorism crosses borders easily and may directly affect the American homeland. That was evident in the New York World Trade Center bombing in 1993, and more recently in the activities around the turn of the century. The terrorist bombings of the U.S. garrison at Khobar Towers, Saudi Arabia, the two U.S. embassies in East Africa, and the recent USS *Cole* incident, also illustrate the reach of terrorists against U.S. interests and the profound domestic implications they pose.

To be functionally comprehensive, the national strategy should address the full spectrum of the nation's efforts against terrorism: intelligence, deterrence, prevention, investigation, prosecution, preemption, crisis management, and consequence management. Our nation's highest goal must be the deterrence and prevention of terrorism. The United States cannot, however, prevent all terrorist attacks. When deterrence and prevention fail, the nation must respond effectively to terrorism, whether to resolve an ongoing incident, mitigate its consequences, identify the perpetrators, and prosecute or retaliate as appropriate. The national strategy should deal with all aspects of combating terrorism and must carefully weigh their relative importance for the purpose of allocating resources among them.

The national strategy should apply to the nation as a whole, not just the Federal Executive Branch. The Federal government should lead a strategic planning process that involves States and communities as essential and equal partners.

The national strategy must be appropriately resourced, by all levels of government, to provide a reasonable opportunity to achieve its successful implementation. At the Federal level, that will require a closer relationship between the Executive and Legislative Branches. Nationally, that will require better coordination with State and local governments.

ARTICULATING THE END STATE: NATIONAL GOALS

The first step in developing a coherent national strategy is for the Executive Branch to define some meaningful, measurable expression of what it is trying to achieve in combating terrorism. The Federal government's goals have previously been expressed primarily in terms of program execution. Administrative measurements alone do not foster effective management of a national program.

The national strategy must express preparedness goals in terms of an "end state" toward which the program strives. Since there exists no ready-made measurement of a country's preparedness for terrorism, especially domestically, the Executive Branch must develop objective measurements for its program to combat terrorism, to track its progress, to determine priorities and appropriate funding levels, and to know when the desired "end state" has been achieved.

The nation's strategy for combating terrorism requires results-based goals for three reasons. First, the programs need an end-state goal. Elected and appointed officials from Federal, State, and local governments must be able to allocate resources to specific geographic regions according to requirements of that region. Re-

sources should be allocated to achieve that broadest application for all emergency and disaster needs, consistent with preparedness goals. That approach is fundamental to the principles of building on existing systems and to achieving the maximum possible multipurpose capability.

Second, programs for combating terrorism need accountability. Legislators and public officials, especially elected ones, must have some reliable, systematic way of assessing the extent to which their efforts and taxpayers' money are producing effective results. The performance and results of programs for combating terrorism are currently assessed almost solely according to anecdote. The only concrete measure available at the moment is the dispersal of Federal funds-a process measurement that does not achieve effective strategic management.

Third, programs for combating terrorism need clear priorities. It is impossible to set priorities without first defining results-based objectives. The essence of any coherent strategy is a clear statement of priorities that can be translated into specific policy and programmatic initiatives. Priorities are the transmission mechanism that connects ends to means.

FOSTERING THE MEANS OF STRATEGY: PROGRAM STRUCTURE AND PRIORITIES

Setting priorities is essential in any strategy, but priorities require clear, resultsbased objectives. With some meaningful sense of objectives, it will be possible to develop coherent priorities and an appropriate set of policy prescriptions. For instance, should the nation seek a different level of preparedness for large urban centers than for rural areas? What should be the relative importance of preparing for conventional terrorism, radiological incidents, chemical weapons, biological weapons, or cyber attacks? Should the nation seek to improve its preparedness more against the types of attacks that are most likely to occur, such as conventional terrorist bombings or the use of industrial chemicals, or for those that are most damaging but less likely to occur, such as nuclear weapons or military-grade chemical or biological weapons? With respect to biological weapons, which pathogens deserve priority? Should the emphasis be on smallscale contamination attacks as opposed to large-scale aerosol releases of the worst pathogen types, such as anthrax, plague, and smallpox? What is the relative priority for allocating resources to protect critical infrastructure, especially from cyber attacks?

The answers to these and other questions have important implications for the allocation of resources for training, equipment acquisition, exercises, research and development, pharmaceutical stockpiles, vaccination programs, and response plans. A coherent national strategy would provide clarity to the allocation of resources across the full range of possible activities to combat terrorism. To date, these critical resource allocation decisions have been made in an ad hoc manner and without reference to meaningful national goals.

We cannot stress strongly enough that the strategy must be truly national in character-not just Federal. The approach to the domestic part of the national strategy should, therefore, be "bottom up," developed in close coordination with local, State, and other Federal entities.

Mr. Chairman, for those and other reasons, we believe that it is time to craft a national strategy for combating terrorism to guide our efforts-one that will give our citizens a level of assurance that we have a good plan for dealing with the issue; one that will provide State and local governments with some direction that will help them make decisions that will contribute to the overall national effort; one that will let our potential adversaries know, in no uncertain terms, how serious we are.

THE NATIONAL OFFICE FOR COMBATING TERRORISM

"The United States has no coherent, functional national strategy for combating terrorism; and the next President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office."

To many at the State and local levels, the structure and process at the Federal level for combating terrorism appear uncoordinated, complex, and confusing. Our first report included a graphical depiction of the numerous Federal agencies and offices within those agencies that have responsibilities for combating terrorism. I have provided additional copies of those charts to the Members of the subcommittee as one way of illustrating the level of complexity.

Attempts to create a Federal focal point for coordination with State and local officials—such as the National Domestic Preparedness Office—have been only partially successful. Moreover, many State and local officials believe that Federal programs intended to assist at their levels are often created and implemented without consulting them. Confusion often exists even within the Federal bureaucracy. The current coordination structure does not possess the requisite authority or accountability to

make policy changes and to impose the discipline necessary among the numerous Federal agencies involved.

For those and other reasons, we recommended the establishment of a senior level coordination entity in the Executive Office of the President, entitled the "National Office for Combating Terrorism," with the responsibility for developing domestic and international policy and for coordinating the program and budget of the Federal government's activities for combating terrorism. The title of the entity is not as important as its responsibilities, the functions that it will be called upon to perform, and the structure and authorities that we believe, at a minimum, such an entity must have.

RESPONSIBILITIES AND FUNCTIONS

1. National Strategy. Foremost will be the responsibility to develop the comprehensive national strategy described above. That strategy must be approved by the President and updated annually.

2. Program and Budget. A concurrent responsibility of the National Office for Combating Terrorism will be to work within the Executive Branch and with the Congress to ensure that sufficient resources are allocated to support the execution of the national strategy. The U.S. strategy for deterrence, prevention, preparedness, and response for terrorists acts outside the United States, developed under the leadership of the Department of State, is comprehensive and, for the most part, appropriately resourced. It is on the domestic front that much additional effort and coordination will be required. The Executive should provide comprehensive information to the Congress to consider in the deliberative authorization and appropriations processes. In addition to a comprehensive strategy document, supporting budget information should include a complete description and justification for each program, coupled with current and proposed out-year expenditures.

3. Intelligence Coordination and Analysis. We recommended that the National Office for Combating Terrorism provide coordination and advocacy for both foreign and domestic terrorism-related intelligence activities, including the development of national net assessments of terrorist threats. A critical task will be to develop, in concert with the Intelligence Community—including its Federal law enforcement components—policies and plans for the dissemination of intelligence and other pertinent information on terrorist threats to designated entities at all levels of government—local, State, and Federal. To oversee that activity, we recommended that an Assistant Director for Intelligence in the National Office direct the intelligence function for Combating Terrorism, who should be "dual-hatted" as the National Intelligence Officer (NIO) for Combating Terrorism at the National Intelligence Council. That Assistant Director/NIO and staff would be responsible for compiling terrorism intelligence products from the various agencies, for providing national-level threat assessments for inclusion in the national strategy, and for producing composite or "fused" products for dissemination to designated Federal, State, and local entities, as appropriate. That person will serve as focal point for developing policy for combating terrorism intelligence matters, keeping the policymaking and operational aspects of intelligence collection and analysis separate. The Assistant Director will also be the logical interface with the intelligence oversight committees of the Congress. It is, in our view, important to have a senior-level position created for this purpose. To assist in this intelligence function, we also recommended the establishment of a "Council to Coordinate Intelligence for Combating Terrorism," to provide strategic direction for intelligence collection and analysis, as well as a clearance mechanism for product dissemination and other related activities. It should consist of the heads of the various Intelligence Community entities and State and local representatives who have been granted appropriate security clearance.

4. Plans Review. We recommended that the National Office for Combating Terrorism be given authority to review State and geographical area strategic plans, and at the request of State entities, review local plans or programs for combating terrorism, for consistency with the national strategy. That review will allow the National Office to identify gaps and deficiencies in Federal programs.

5. Proposals for Change. We recommended that the National Office for Combating Terrorism have authority to propose new Federal programs or changes to existing programs, including Federal statutory or regulatory authority.

6. Domestic Preparedness Programs. The National Office should direct the coordination of Federal programs designed to assist response entities at the local and State levels, especially in the areas of "crisis" and "consequence" planning, training, exercises, and equipment programs for combating terrorism. The national strategy that the National Office should develop-in coordination with State and local stake-

holders-must provide strategic direction and priorities for programs and activities in each of these areas.

7. Health and Medical Programs. Much remains to be done in the coordination and enhancement of Federal health and medical programs for combating terrorism and for coordination among public health officials, public and private hospitals, prehospital emergency medical service (EMS) entities, and the emergency management communities. The National Office should provide direction for the establishment of national education programs for the health and medical disciplines, for the development of national standards for health and medical response to terrorism, and for clarifying various legal and regulatory authority for health and medical response.

8. Research, Development, Test, and Evaluation (RDT&E), and National Standards. The National Office should have the responsibility for coordinating programs in these two areas. The national strategy should provide direction and priorities for RDT&E for combating terrorism. We believe that the Federal government has primary responsibility for combating terrorism RDT&E. Moreover, we have essentially no nationally recognized standards in such areas as personal protective equipment, detection equipment, and laboratory protocols and techniques.

9. Clearinghouse Function. We recommended that the National Office for Combating Terrorism serve as the information clearinghouse and central Federal point of contact for State and local entities. It is difficult for local jurisdictions and State agencies, even those with experience in complex Federal programs, to navigate the maze of the Federal structure. The National Office for Combating Terrorism should assume that role and serve as the "one-stop shop" for providing advice and assistance on Federal programs for training, planning, exercises, equipment, reporting, and other information of value to local and State entities.

STRUCTURE AND AUTHORITY

1. Political Accountability and Responsibility. The person designated as the focal point for developing a national strategy and for coordinating Federal programs for combating terrorism must have political accountability and responsibility. That person should be vested with sufficient authority to accomplish the purposes for which the office is created and should be the senior point of contact of the Executive Branch with the Congress. For these reasons, we recommended that the President appoint and the Senate confirm the Director of the National Office for Combating Terrorism, who should serve in a "cabinet-level" position.

2. Program and Budget Authority. The National Office for Combating Terrorism should have sufficient budget authority and programmatic oversight to influence the resource allocation process and ensure program compatibility. That authority should include the responsibility to conduct a full review of Federal agency programs and budgets, to ensure compliance with the programmatic and funding priorities established in the approved national strategy, and to eliminate conflicts and unnecessary duplication among agencies. That authority should also include a structured certification/decertification process to formally "decertify" all or part of an agency's budget as noncompliant with the national strategy. A decertification would require the agency to revise its budget to make it compliant or, alternatively, to allow the agency head to appeal the decertification decision to the President. This limited authority would not give the Director of the National Office the power to "veto" all or part of any agency's budget, or the authority to redirect funds within an agency or among agencies.

3. Multidisciplinary Staffing. The National Office for Combating Terrorism should have full-time multidisciplinary expertise, with representation from each of the Federal agencies with responsibilities for combating terrorism, and with resident State and local expertise. For programs with a domestic focus, the National Office for Combating Terrorism must have sufficient resources to employ persons with State and local expertise and from each of the response disciplines.

4. No Operational Control. While the National Office for Combating Terrorism should be vested with specific program coordination and budget authority, it is not our intention that it have "operational" control over various Federal agency activities. We recommended that the National Office for Combating Terrorism not be "in charge" of response operations in the event of a terrorist attack. The National Office should provide a coordinating function and disseminate intelligence and other critical information. Mr. Chairman, I should note at this point that the word "czar" is inappropriate to describe this office. The Director of this office should not be empowered to order any Federal agency to undertake any specific activity. With few exceptions, we recommended that existing programs remain in the agencies in which they currently reside. One notable exception will be the functions of the National Domestic Preparedness Office (NDPO), currently housed in the Federal Bureau of Inves-

tigation. The new office should subsume all of the *intended* functions of the NDPO-coordination, information clearinghouse, advice and assistance to State and local entities. The National Office for Combating Terrorism should also assume many of the interagency coordination functions currently managed by the National Security Council office of the National Coordinator for Security, Counterterrorism, and Infrastructure Protection. For example, the responsibility for coordination of certain functions related to combating terrorism-Assistance to State and Local Authorities, Research and Development, Contingency Planning and Exercises, and Legislative and Legal Issues, among others-will devolve to the National Office for Combating Terrorism. We also recommended that the National Office for Combating Terrorism absorb certain entities as adjuncts to its office, such as the Interagency Board for Equipment Standardization and InterOperability.

5. Advisory Board for Domestic Programs. To assist in providing broad strategic guidance and to serve as part of the approval process for the domestic portion of strategy, plans, and programs of the National Office for Combating Terrorism, we recommended the establishment of a national "Advisory Board for Domestic Programs." That Board should include one or more sitting State governors, mayors of several U.S. cities, the heads of several major professional organizations, and a few nationally recognized terrorism subject matter experts, as well as senior officials from relevant Federal agencies. The President and the Congress should each appoint members to this board.

ALTERNATIVES CONSIDERED

Mr. Chairman, the members of the Advisory Panel considered a number of alternatives to our recommendation for a National Office of the type that I have described, before coming to the unanimous conclusion that the path we chose was by far the best of the alternatives. Among others considered by the panel was a new Deputy Attorney General, an "enhanced" Federal Emergency Management Agency, the possibility of some other Federal agency, or simply trying to improve upon the *status quo*. I will be pleased to answer questions from Members about our rationale for discounting those alternatives.

CONGRESSIONAL ISSUES

"The Congress shares responsibility for the inadequate coordination of programs to combat terrorism; it should consolidate its authority over programs for combating terrorism into a Special Committee for Combating Terrorism—either a joint committee between the Houses or separate committees in each House—and Congressional leadership should instruct all other committees to respect the authority of this new committee and to conform strictly to authorizing legislation."

The Congress's strong interest in, and commitment to, U.S. efforts to combat terrorism is readily apparent. The Congress took the initiative in 1995 to improve the nation's domestic preparedness against terrorism. But the Congress has also contributed to the Executive Branch's problems. Over the past five years, there have been a halfdozen Congressional attempts to reorganize the Executive Branch's efforts to combat terrorism, all of which failed. None enjoyed the support of the Executive Branch. At least 11 full committees in the Senate and 14 full committees in the House—as well as their numerous subcommittees—claim oversight or some responsibility for various U.S. Programs for combating terrorism. Earmarks in appropriations bills created many of the Federal government's specific domestic preparedness programs without authorizing legislation or oversight. The rapidly growing U.S. budget for combating terrorism is now laced with such earmarks, which have proliferated in the absence of an Executive Branch strategy. The Executive Branch cannot successfully coordinate its programs for combating terrorism alone. Congress must better organize itself and exercise much greater discipline.

The creation of a new joint committee or separate committees in each House is necessary to improve the nation's efforts to fight terrorism. The committee should have a substantial standing staff. The new National Office for Combating Terrorism must establish a close working relationship with the committee, and propose comprehensive and coherent programs and budget requests in support of the new national strategy. The new joint or separate committee should have the authority to dispose of the Executive Branch request and to oversee the execution of programs that it authorizes. For this to work, other Congressional authorizing committees with an interest in programs for combating terrorism must recognize the concurrent, consolidated authority of the joint or separate committee; and relevant appropriations committees must exercise restraint and respect the authorizing legislation of the new structure. We recognize that this task is no less daunting than the Executive Branch reorganization that we propose above, but it is no less needed.

SPECIFIC FUNCTIONAL RECOMMENDATIONS

The focus of the Advisory Panel continues to be on the needs of local and State response entities. "Local" response entities—law enforcement, fire service, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers—will always be the "first response," and conceivably the only response. When entities at various levels of government are engaged, the responsibilities of all entities and lines of authority must be clear.

1. *Collecting Intelligence, Assessing Threats, and Sharing Information.* The National Office for Combating Terrorism should foster the development of a consolidated all-source analysis and assessment capability that would provide various response entities as well as policymakers with continuing analysis of potential threats and broad threat assessment input into the development of the annual national strategy. That capability should be augmented by improved human intelligence collection abroad, more effective domestic activities with a thorough review of various Federal guidelines, and reasonable restrictions on acquisition of CBRN precursors or equipment. The National Office should also foster enhancements in measurement and signature intelligence, forensics, and indications and warning capabilities. To promote the broadest possible dissemination of useful, timely (and if necessary, classified) information, the National Office should also oversee the development and implementation of a protected, Internet-based single-source web page system, linking appropriate sources of information and databases on combating terrorism across all relevant functional disciplines.

2. *Operational Coordination*. The National Office for Combating Terrorism should encourage Governors to designate State emergency management entities as domestic preparedness focal points for coordination with the Federal government.

The National Office should identify and promote the establishment of singlesource, "all hazards" planning documents, standardized Incident Command and Unified Command Systems, and other model programs for use in the full range of emergency contingencies, including terrorism. Adherence to these systems should become a requirement of Federal preparedness assistance.

3. *Training, Equipping, and Exercising*. The National Office for Combating Terrorism should develop and manage a comprehensive national plan for Federal assistance to State and local agencies for training and equipment and the conduct of exercises, including the promulgation of standards in each area. The National Office should consult closely with State and local stakeholders in the development of this national plan. Federal resources to support the plan should be allocated according to the goals and objectives specified in the national strategy, with State and local entities also providing resources to support its implementation.

4. *Health and Medical Considerations*. The National Office for Combating Terrorism should reevaluate the current U.S. approach to providing public health and medical care in response to acts of terrorism, especially possible mass casualty incidents and most particularly bioterrorism. The key issues are insufficient education and training in terrorism-related subjects, minimum capabilities in surge capacity and in treatment facilities, and clear standards and protocols for laboratories and other activities, and vaccine programs. A robust public health infrastructure is necessary to ensure an effective response to terrorist attacks, especially those involving biologic agents. After consultation with public health and medical care entities, the National Office should oversee the establishment of financial incentives coupled with standards and certification requirements that will, over time, encourage the health and medical sector to build and maintain required capabilities. In addition, Federal, State, and local governments should clarify legal and regulatory authorities for quarantine, vaccinations, and other prescriptive measures.

5. *Research and Development, and National Standards.* The National Office for Combating Terrorism should establish a clear set of priorities for research and development for combating terrorism, including long-range programs. Priorities for targeted research should be responder personnel protective equipment; medical surveillance, identification, and forensics; improved sensor and rapid readout capability; vaccines and antidotes; and communications interoperability. The National Office must also coordinate the development of nationally recognized standards for equipment, training, and laboratory protocols and techniques, with the ultimate objective being official certification.

6. *Providing Cyber Security Against Terrorism*. Cyber attacks inside the United States could have "mass disruptive," even if not "mass destructive" or "mass casualty" consequences. During the coming year, the Advisory Panel will focus on specific aspects of critical infrastructure protection (CIP), as they relate to the potential for terrorist attacks. In our discussions thus far, we have identified several areas for further deliberation, including CIP policy oversight; standards; alert, warning,

and response; liability and other legal issues, and CIP research. We will make specific policy recommendations in our next report.

Areas of Agreement and Disagreement with the Report of The National Commission on Terrorism

Mr. Chairman, the charters and objectives of the Bremer Commission and the Gilmore Commission are, for the most part, very different. The Bremer Commission focused on international terrorism. The Gilmore Commission's clear mandate is on domestic preparedness-deterring, preventing, and responding to terrorist incidents inside the borders of the United States.

There are, nevertheless, several overlapping areas of interest between the two reports and the attendant findings and recommendations.

Both panels agree on the increasing nature of the threat of international terrorism, including the potential for more attacks from international groups inside the borders of the United States.

Both panels specifically agree that certain measures must be taken to improve intelligence collection and dissemination on terrorists, including:

- Repealing the 1995 Director of Central Intelligence Guidelines as they apply to recruiting terrorist informants
- Reviewing and clarifying, as may be indicated, the Attorney General's Guidelines on Foreign Intelligence Collection and the Guidelines on General Crime, Racketeering Enterprise, and Domestic Security/Terrorism Investigations
- Directing the Department of Justice Office of Intelligence Policy and Review not to require a process for initiating actions under the Foreign Intelligence Surveillance Act that are more stringent than those required by the statute

Both panels agree that significant improvements must be made in the ability of intelligence and law enforcement agencies to collect, analyze, disseminate and share intelligence and other information more effectively.

Both panels agree that there must be a comprehensive strategy or plan for dealing with terrorism, including the ways in which both the Executive Branch and the Congress develop and coordinate program and budget processes.

Both panels agree in principal that the Department of Defense (DoD) and U.S. Armed Forces may have a major role in preventing or responding to a terrorist attack, especially one involving a chemical, biological, radiological or nuclear device. We likewise strongly agree that insufficient planning, coordination, training, and exercises have been developed and implemented for the possibility of major DoD and military involvement. The one area in which we disagree has to do with "lead agency." The Bremer Commission suggests that a response to a catastrophic attack may indicate the designation of DoD as Lead Agency. While we agree that DoD may have a major role, we firmly believe that the military must always be directly under civilian control. As a result, we recommend that the President always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency. Many Americans will not draw the technical distinction between the Department of Defense-the civilian entity-and the U.S. Armed Forces-the military entity. Although the Department of Defense and every major component of that department have civilian leaders, the perception will likely be that "the military" is in the lead. This recommendation does not ignore the fact that the DoD, through all of its various agencies-not just the Armed Forces-has enormous resources and significant capabilities for command, control, communications, intelligence, logistics, engineer, and medical support and may play a major role in response to a terrorist attack, especially one with potentially catastrophic consequences. Those resources can still be brought to bear but should, in our view, always be subordinated to another civilian agency.

Summary

Mr. Chairman and Members of the subcommittee, the members of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction are convinced that the essence of its recommendations are essential to the national effort to combat terrorism: the promulgation of a truly national strategy; the appointment of a senior person at the Federal level who has the responsibilityimportantly, who can be seen as having the responsibility-for coordinating our national efforts; improvements in the way Congress addresses this issues; and the implementation of the functional recommendations dealing with:

- improving intelligence, threats assessments, and information sharing;
- better planning, coordination and operations;
- enhanced training, equipping, and exercising;

- improving health and medical capabilities;
- promoting better research and development and developing national standards;
- enhancing efforts to counter agroterrorism; and
- improving cyber security against terrorism.

With the exception of the one dissent on the issue of a lead role for the military, our recommendations are as firmly unanimous as we believe that they are reasonable and specific.

This is not a partisan political issue. It is one that goes to the very heart of public safety and the American way of life. We have members on our panel who identify with each of the major national political parties, and represent views across the entire political spectrum. We urge Members on both sides of the aisle, in both Houses of the Congress, to work with the Executive Branch to bring some order to this process and to provide some national leadership and direction to address this critical issue. Thank you again for this opportunity.

Chairman KYL. Thank you very much, General. There is so much that we will get into as we pull pieces out of your report that we think might help us to legislate in the area.

Let me first of all address something that you said because I think it is recognized by all of us here in Congress. We have talked about it, that our failure to organize Congress in a coherent and focused way on the problem is somewhat a mirror image of our view that the administration hasn't focused very well either.

It might be the fact that we have the same kind of operational issues; that is to say, our appropriations people are the operational group for funding. The Judiciary Committee, of which this is a subset, is the operational group with respect to changing the law and evidentiary gathering or sharing, and so on. The Intelligence Committee, of which I am a member, has certain other operational functions.

However, that isn't to suggest that we couldn't create a select Committee along the lines of the Intelligence Committee which would pluck people from each of those operational committees to provide the same kind of oversight that you are suggesting would be appropriate at the executive level, and I think that is something that we are going to try to pursue.

Let me just ask you this general question to begin. When people think of trying to prepare for terrorism, we divide the issue into two parts; No. 1, preventing it, the intelligence-gathering, the other kinds of things that we will talk a little bit more about, and then the aftermath, the response.

As to that second aspect of it, there seems to be a sense, at least in the people that I have talked to, that while it is inevitable that there will be terrorist actions here in the United States, and while we can generally try to prepare at least the first responders in our largest communities on how basically to respond to these kinds of emergencies and perhaps even given them some equipment that would be unique to the kinds of challenges they might fact, the reality is that the country is so big, the opportunities so great in so many different places that it would be impossible to adequately prepare in every potential community for every potential threat. Therefore, there seems to be just sort of a general throwing up of the arms of what can we really do.

How do you respond to that sense of almost a sense that we really can't do much about it if, in fact, the terrorist event occurs, except to have some general agency in Washington that would direct the response of the local entities to the extent they needed help?

General CLAPPER. Well, sir, I think there are capabilities already resident in the Government which can be embellished, coordinated better, where we can be certainly in a better posture to respond. I think more can be done from an intelligence perspective in the context of prevention.

A lot of great work is going on as we speak. I think the CIA and the FBI—I discussed this earlier today—have made giant strides in their recognition of the fact that the jurisdictional boundaries are not always respected by terrorists.

If, in fact, our ability to detect and preempt an attack fail, then I think there is more that can be done to respond. What we have in mind here are exercises, training, equipment, standards, medical coordination. There is a lot of just sort of grunt work that if the commitment is made to do it could be done which would put us in a better posture to respond.

To say that if we spend "x" billions of dollars or take some sort of administrative action, that that will provide an iron-clad guarantee to the citizenry that we will never be confronted with a terrorist attack is obviously unrealistic. But we can certainly do more to posture ourselves to detect the potential for terrorism, acknowledging the fact that in the context of terrorism we are always going to be dealing with ambiguous intelligence, but also be prepared to respond.

Now, the reason this is important, in my view, is because if we do that, that in itself serves as a form of deterrence. If we have a capability after the fact, for example, the forensic capability to determine a return address, to use the phrase, of a terrorist and the terrorist knows that and that we will, if we determine who did it, reach out and touch, that has a very compelling message and, as I say, serves as a deterrent.

So I think there are things we can do to put ourselves in a better posture, but to say that that will ensure that we are never attacked, no, sir, we can't do that.

Chairman KYL. Well, I think there is—I don't want to use the word a sense of fatalism, which is what I started to say before, but a sense that while you can train to a certain level to respond, once it has gotten to that point our abilities are significantly limited. That is why I tend to focus, plus the fact that this committee's jurisdiction is more focused on the prevention side, the intelligence-gathering, the intelligence-sharing, and so on.

I would like to get to some of your recommendations with respect to sharing of intelligence which you just alluded to between the FBI and the CIA. In this country, of course, the FBI is much more limited in what it can do than the CIA would be in gathering intelligence abroad, for example, and that puts some limits on what the FBI feels it can share, particularly if it has got an ongoing investigation in terms of what it can share with the CIA or with other agencies.

Would you speak to that and the recommendations of the panel?

General CLAPPER. Well, sir, I don't know that I have anything new and profound and dramatic, other than to endorse what is already going on. An example is the formation and organization of the Counterterrorism Center, which is an intelligence community entity which involves all the intelligence community agencies, to

include the FBI, which is a structural mechanism to ensure visibility and coordination between and among the intelligence agencies.

The important thing to me is that I think we have to be mindful and sensitive to the legal boundaries between the purview of the FBI in collecting domestic intelligence and the purview of the intelligence community in collecting and using foreign intelligence, and the relationship of those two activities as it applies to protection of our civil liberties, et cetera.

So I think those sensitivities have to be attended to, but at the same time we need to ensure that the information baton is not dropped as it is handed off in the case of terrorism which originates overseas from a foreign source but is reaching out and touching us domestically in the United States. I think the mechanisms and the structures and organizations and the processes that the FBI and CIA have come up with go a long way toward doing that.

An issue where I think we can improve is in the area of dissemination. I think there are mechanisms that we can establish whereby certain State and local officials in certain conditions should be afforded access to any of this intelligence if it affects their jurisdiction.

In my active duty days as an intelligence officer, I was involved in or presided over many, many intelligence exchanges with our friends and allies. It seems to me if we can build mechanisms to do that, we can certainly build mechanisms whereby intelligence can flow to, say, State Governors or the senior emergency planner in each State or other senior fire, rescue, et cetera, people who need to have access to that kind of information. Now, if that entails some sort of a special classification system or whatever, then that is fine. We should do that. We have it within our capability and it is strictly essentially a policy issue.

Another thing I have been a proponent of is capitalizing on a system I think you may be familiar with, sir, in the intelligence community called InteLink, which is roughly analogous to the intelligence community's very own internet. I have been a proponent for exporting this same kind of thing to the so-called first responder community on a selected capability.

One of the recurrent themes that we have heard in our dialogs with State and local people over the last couple of years is a hunger or thirst or requirement for threat information, and we have made some recommendations on how we think that can be effected. So I think in the areas of coordination between the two agencies, focusing more on the analytic capability, and most importantly of all, I think, is disseminating information, where appropriate, to selected State and local officials.

Chairman KYL. Let me just ask you two more questions here, both related to that. Last year, Senator Feinstein and I both cosponsored a bill that would have clarified current law regarding the ability of the FBI and the Justice Department to share certain criminal wiretap information pertaining to terrorism with the CIA and other Government agencies.

Did the Commission discover any instances where law enforcement information was not shared due to legal interpretations about

the FBI and Justice Department's ability to share information with other Government agencies?

General CLAPPER. Sir, I can't off the top of my head come up with specific cases in point. I will tell you, though, that we heard in the case of the application of the FISA law where it was the feeling of some that although the requests for FISA authorizations were not turned down, the bar was set pretty high for them to even be entered into in the first place. That is the genesis of the recommendation that I mentioned earlier in my oral statement about not going beyond the provisions of what is in the statute.

I might also comment on the DCI guidelines that were promulgated in about the 1995 timeframe. I was a member of the Downing Assessment Task Force that investigated the Khobar Towers bombing in 1996, which parenthetically was an epiphany experience for in terms of when I actually got religion about terrorism and what it can do.

I discovered a whole host of both administrative and legislatively derived restrictions and rules on the kinds of people who can be recruited to collect information. Each one of these is well-intended and probably came out of some abuse, at least as viewed by some, of engaging some nefarious person to collect information on nefarious activities.

The impact, though, on the collector force, if I could call it that, is kind of chilling because of this litany of restrictions that apply to the collection of foreign intelligence. So the set of recommendations we made about looking at all these rules and regulations as they pertain to the collection of information on terrorism—both we and other panels, particularly Ambassador's panel, have strongly urged review and in some cases relaxation of some of these strictures.

Chairman KYL. Let me just follow up with a question on that precise point. Former Director Woolsey, a member of that panel, drew the distinction between recruitment of agents against another government and recruitment of agents or sources with respect to terrorism. That commission didn't recommend a relaxation of the standards as opposed to recruitment against another government, but with respect to terrorism made the point that you are dealing with, by definition, a group of people who have nefarious backgrounds and those restrictions should be relaxed.

Do you generally concur with that personally and is that the view of the panel?

General CLAPPER. Yes, sir, I do, and it is the view of the panel. I would cartoon this a little bit, but I have said in other fora that if you want to restrict yourself to the likes of Mother Teresa and that is who you are going to recruit information from, then that will certainly shape the kind of information you get.

We have to be prepared to deal with very nasty, nefarious people who by definition do bad things. And if we want to have any hope of gaining insight into what they are doing, then we are going to have to take the risk that we will, in fact, engage with some pretty nasty people. So the short answer is yes.

Chairman KYL. Did your panel acquire any information which would be useful to share with us in a closed setting, any specific

examples or specific conversations with people that would be useful to us that we could talk about?

General CLAPPER. Yes, sir, we could, and I would recommend, to take advantage of this dual membership of Ambassador Jerry Bremer, that he would be involved in those discussions.

Chairman KYL. I think we would like to call upon you to get your advice on that because when Senator Feinstein and I put together our bill at the end of last year, we originally had that recommendation in the bill and due to opposition from at least one member of this committee, that provision was dropped. So I think we need to hone in on that.

There is a lot more I could get into, but I really want to hear from our second panel, as well, and I don't know when we are going to be having the next vote. So let me offer an opportunity for you to add anything else you would like to add in writing. We will leave the time of this hearing open for, say, 3 days should you want to do that or should any member of the Subcommittee wish to ask you a question and have you respond to it.

I really appreciate your testimony here, and we will be looking forward to getting back with you and Governor Gilmore when we begin to put our legislation together.

Thank you very much, General Clapper.

General CLAPPER. Thank you, sir.

Chairman KYL. Let me ask our second panel if they would please come forward.

As I said earlier, our second panel is made up of distinguished scholars: Dr. Anthony Cordesman, of the Center for Strategic and International Studies, and Dr. Yonah Alexander, of the Potomac Institute.

Both of you gentlemen bring a wealth of expertise on the subject of terrorism and I personally thank you very much for your willingness to appear before the subcommittee.

Dr. Cordesman, let's begin with you. As I indicated earlier, we will make your prepared remarks a part of our record, and if you would like to summarize those remarks without any time limitation I would be happy to receive that at this time.

STATEMENT OF ANTHONY H. CORDESMAN, ARLEIGH A. BURKE CHAIR IN STRATEGY, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, WASHINGTON, D.C.

Mr. CORDESMAN. Thank you very much, Senator, and I thank the Subcommittee for the opportunity to testify this afternoon. I do have some prepared remarks and I appreciate having them included in the record. I know you have a lot of questions, so let me begin with a few brief introductory remarks.

In the work that we did on this subject in the CSIS, we encountered a number of problems that I think you are going to have to address over the next few years. One was the decoupling of asymmetric warfare and terrorism. This was much less apparent in the Department of Defense than in the other branches of Government, but if you look at the record, you find again and again the conclusion is drawn that because today's terrorists are not supported by states, they will not use biological or nuclear weapons or use ad-

vanced technology effectively in ways which could saturate response capabilities at the Federal, State, and local level.

But as you mentioned at the beginning of this hearing, we are also dealing with states like North Korea, Iraq, and Iran, and there will be more in the future. And I think by sizing so much of our response effort around terrorists without state support, we may risk creating a response and intelligence effort which deals with the wrong threat and perhaps the less important threat.

This permeates a lot of what goes on in individual civil agencies. It is striking that we are spending some $11 billion trying to deal with the threat of counterterrorism on the record, but when you disaggregate that money, a good $7 billion of it goes to the physical protection of Federal facilities and of U.S. military overseas, and the actual budget going into dealing with counterterrorism is often very limited.

I think one thing that is also striking is the tendency to freeze our perceptions around today's technology. We do not at this point in time face a growing threat statistically in terms of the number of attacks or casualty levels, but we do face a radical process of technological change.

One aspect of this is attacks on information systems, the growing vulnerability of a more integrated infrastructure. A key area is the risk of biotechnology and biological weapons, which is an area where many countries, and indeed many well-organized terrorist movements in the future may be able to use advances in biotechnology or food processing equipment or pharmaceuticals, to use methods of attack which frankly we are not even preparing for because the biological threats we deal with are the ones fundamentally we already understand. We also face the problem over time that nuclear weapons or nuclear devices may become more available. We have not really looked at those risks.

There is another problem that strikes me. It is so easy to talk about strategy and organization that often we do not look at the problem of vulnerability. Yet, vulnerability is changing along with the methods of attack. Our vulnerability in terms of information systems is one example. Our vulnerabilities in terms of specific types of biological attack and nuclear attack is another.

We tend to warn in very broad, generic terms about methods of attack, but our data on weapons effects often date back to the early 1970's. In some cases like biological weapons, I can recognize them because I was then the DRPA program manager for biological weapons, and it is very disturbing to see them repeated some 30 years later when at least then we knew how uncertain and unreliable many of these data were. If we tailor our response around that kind of planning, we risk providing the wrong templates and the wrong models at the Federal, State, and local level.

Last, let me make a point based, I think, on all too much experience in Washington. I think you yourself can remember previous calls for strategy and legislation that we needed to have a national strategy document, and that there should be a Department of Defense strategy document. Well, those documents are issued every year. No one knows what they mean, no one uses them, no one can figure out what their impact is on a single program or a single area

of our budget. We have had a drug czar, and whether or not that has really shaped effective programs is, to put it mildly, debatable.

The point I would raise in closing is this: Unless you really concern yourself about developing effective future-year programs, program budgets, clear ways to assess the effectiveness of programs in intelligence, defense, and response, both in terms of foreign intelligence and the fusion of law enforcement, we risk doing what we always do in Washington. We mandate another strategy document; we put someone in charge of something or we create at least a new office somewhere in the Federal Government. And 2 years later, none of us can figure out what we accomplished.

The old routine in Washington that you have to follow the money is just as important in intelligence, counterterrorism, and dealing with weapons of mass destruction as it is in any other area.

Thank you.

[The prepared statement of Mr. Cordesman follows:]

STATEMENT OF ANTHONY H. CORDESMAN, ARLEIGH A. BURKE CHAIR IN STRATEGY, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, WASHINGTON, D.C.

"Terrorism" is a topic that arouses so much fear and revulsion that there is a natural tendency to "cry wolf," and to confuse the potential threat with one that is actually occurring. Similarly, any discussion of the new threats posed by weapons of mass destruction and information warfare involves threats that are so serious that there is an equal tendency to respond like Chicken Little and worry that the sky is falling.

This scarcely means we should not be worried about terrorism. The potential threats to our society are all too real. Democratic societies are inherently vulnerable. They place few controls over their borders, their citizens, or foreigners who have actually entered their territory. This is particularly true of the US, and there are many vulnerable points in our social structure and economy that foreign governments and extremist movements, domestic extremists and the mentally ill can attack.

There equally are good reasons to be increasingly concerned about new forms of asymmetric warfare and terrorism, and the use of new and more lethal forms of technology.

Yet, there are equally good reasons to be careful about exaggerating the threat, and being careless about the way we define it. We can improve intelligence, defense, and response in many ways. We can anticipate future risks, even if we cannot predict the future. We do, however, have limited resources and competing priorities, and we face daunting uncertainties about the nature of the problem terrorism poses to our security.

CRYING WOLF MEETS CHICKEN LITTLE

It is not easy to characterize the threat - at least in unclassified terms. There are grave weaknesses and shortcomings in the statistics that the US government makes publicly available on terrorism. We do not have an adequate picture of the number, type, and seriousness of domestic incidents, and it is often difficult to separate out criminal activity, threats, actual action by domestic terrorists, and the actions of mentally disturbed individuals.

The data the US government publishes on international terrorist activity also has many defects. Much of it is highly over-aggregated, and does not provided anything approaching sophisticated pattern analysis. We stress international terrorism, but ignore largely foreign domestic violence that may generate terrorism in the future. We tend to demonize known terrorist groups, but ignore or underplay the capability of foreign states to conduct covert operations or use proxies to do so.

We exaggerate the existence of foreign networks, such as Usama Bin Ladin, and understate the risk that individual terrorist elements may lash out against us in ways we do not expect. Much of our analysis is grossly ethnocentric: It assumes that we are the key target of attacks which generally grow out of theater tensions and conflicts where we become a target—if at all—because of our ties to allies and peacekeeping missions.

The fact is, however, that if one looks at the recent patterns in terrorism, the US is no more subject to such attacks today—whether measured in numbers of inci-

dents or casualties—than in the past. The net threat also remains a small one in actuarial terms. The word "terrorism" may trigger a great emotional reaction, but actual casualties and losses are almost actuarially insignificant. Far more people die of traffic accidents on a bad weekend than dies annually of terrorism.

The idea that the end of the Cold War has somehow created a more unstable and violent world is a myth. The world is, has always been, and will remain a violent place. According to the Department of Defense, there have been some 20–30 serious regional conflicts and civil wars going on every day of every year since the end of World War II. We did indeed relate many of these conflicts to the Cold War while it was going on, but in truth, most such conflicts dragged in the superpowers and were not caused by them.

With the exception of the Balkans, we do not see new major regional patterns of violence we can relate to the Cold War. In fact, the end of the Cold War has simply allowed us to focus on the broad realities of ongoing global violence rather than a single threat.

We need to be equally careful about exaggerating the new trends in technological vulnerability. Some of these trends are very real, but our critical infrastructure has always been vulnerable. Nature and chance have shown that repeatedly, and studies done back in the 1950s and 1960s showed how limited attacks—then postulated to be by attackers like the Soviet Spetsnaz—could cripple our utilities, paralyze critical military installations, or destroy our continuity of government. We have always been vulnerable to a truly well-organized terrorist or covert attack.

The fact that there are real wolves in the world, and that the sky can fall—at least—to the extent that far more serious damage is possible than we have ever suffered from in the past—is not a reason to cry wolf or play the role of chicken little.

THE CHANGING FACE OF TERRORISM AND TECHNOLOGY

In saying this, I am all too well aware that no victim of terrorism, or their loved ones, are going to be consoled by the fact that they are a relatively small statistic. The political symbolism of successful terrorist attacks is also often far greater than the casualties, and even an empty threat can help to undermine the fabric of social trust upon which our democracy is based.

Equally important, the fact we have not yet encountered an attack in the US as serious as the strikes on our Embassies in Kenya and Tanzania, or as potentially threatening as Aum Shinrikyo, is in no way a guarantee for the future. Rather than exaggerate current threats, we need to be very conscious of the fact that the nature and seriousness of the threat can change suddenly and with little warning.

Let me give some specific examples:

- At present the US government focuses most of its intelligence analysis, defense planning and response, around a relatively narrow definition of terrorism. It focuses on independent terrorist groups, and not on the threat states can pose in asymmetric warfare. Yet, it is states that have the most access to weapons of mass destruction—particularly biological and nuclear weapons—and which have the most capability to launch sophistication attacks on our information systems.

We face current potential threats from nations like Iran, Iraq, Libya, and North Korea. We can face new threats as a result of our regional alliances and commitments every time a major conflict, crisis, or peace-keeping activity takes place.

Acts can come in the context of over asymmetric warfare, covert state-launched attacks, or the use of terrorist and extremist groups as proxies. Attacks can be made on our allies, our forces and facilities overseas, on US economic interests, or on our own territory. They can involve attackers with very different values, escalation ladders and perceptions and who lash out in a crisis.

This is also one area where the world has really changed since the end of the Cold War. We have always been a natural target because of the sheer scale of our global commitments and interest. Now, however, there is no Soviet Union our potential opponents can turn to, and they have no way of offsetting our advantage in conventional warfare.

We need to bridge the gap between the way in which the US government prepares for asymmetric warfare and to deal with the threat of terrorism—not only in terms of intelligence analysis, but our defense and response planning for Homeland Defense. We also must include intelligence analysis of capabilities and not just intentions. History shows us that the fact that foreign countries and leaders are deterred, or show restraint today, is no guarantee they will behave the same way under crisis conditions.

We need to ensure the effective fusion of intelligence community efforts, military planning, and civil defense and response planning. We should not leave any gap where the Department of Defense seriously plans for large-scale nuclear and biologi-

cal attacks and civil Departments and Agencies focus on relatively lowlevel conventional explosives and limited chemical attacks.

We need to be equally careful not to compartment our analysis of information warfare so that the Department worries about true information warfare while civil departments and agencies worry about hacking and cracking at much lower levels of threat.

Finally, we need to consider the full implications of our call for missile defense, and of our counterproliferation activities. The more we succeed in blocking overt threats, the more we will drive states towards finding alternative means of attack. It makes little sense to close the barn door and leave the windows open.

We need to focus on key areas of technological change. We cannot yet predict what technical capabilities hostile states, extremists and movements will acquire over the next 15–25 years. We can, however, predict that there are several major areas of technological change that can radically alter the effectiveness of asymmetric and terrorist attacks and which require care attention from the intelligence community:

- *The vulnerability of our critical infrastructure is changing:* Our financial systems, communications systems, utilities, and transportation nets are far more tightly integrated than in the past, and we rely far more on national and regional systems, rather than large autonomous local ones. This reduces vulnerability in some ways, but increases vulnerability in others. Systems netting and integration involves shifts in technology that need careful examination.
- *Information systems create new vulnerabilities:* It is all too possible to grossly over-exaggerate our dependency on information systems, their vulnerability, and the difficulty in finding work-grounds, and reconstituting critical systems. Many statements are being made that have no real analytic underpinning and the importance of given systems is poorly researched. The Internet, in particular, is being glamorized to the point of absurdity. Nevertheless, information systems have become part of our critical infrastructure, and virtually invisible cyberattacks may prove to be more lethal in some cases than high explosives. New physical methods of attack, such as EMP weapons, may also be becoming more practical.
- *Chemical weapons and toxins are changing:* It is impossible to discuss fourth generation chemical weapons in an unclassified forum, but the threat has been openly raised by Department of Defense officials. The technology and equipment for older types of chemical weapons is also proliferating at a civil level and becoming steadily more available to governments, extremist movements, and individuals.
- *Biological weapons are changing:* It has been possible to make dry storable biological weapons with nuclear lethality since at least the late 1950s. Advances in biotechnology, food processing equipment, pharmaceuticals, and other dual-use facilities and technologies are also proliferating at a civil level and becoming steadily more available to governments, extremist movements, and individuals. These problems are compound by the rapid spread of expertise and equipment for genetic engineering. The end result is that the technology of attacks on humans, livestock, and crops is becoming steadily more available, and in forms which not only can be extremely lethal and/or costly, but difficult to attribute to a given attacker.
- *The availability of nuclear weapons may change:* It is far too soon to say that broad changes are taking place in the nuclear threat. Nevertheless, the break up of the FSU, and proliferation in India and Pakistan, does create a growing risk that fissile material may become more available for "dirty" and low yield weapons, and the knowledge of how to make crude nuclear devices, handle the high explosives, provide neutron initiators, and deal with the complex triggering problems is also spreading.
- *The risk from radiological weapons may change:* Radiological weapons have not been particularly attractive options in the past. There is, however, a steadily growing mass of nuclear waste, and some studies indicate that the long-term genetic effects of such weapons may be more serious than their short-term effects.
- *The ability to exploit the media and psychological dimension of new technologies has grown: Far more is involved than body counts, physical damage, and economic loss. Even the most limited CBRN or information attack on the US or US targets has great political and psychological impact both within the US and overseas. The spread of mass communications, and use of tools like the Internet and Satellite TV, also increases the impact of attacks. It is all too easy to exaggerate today's threat in each of these areas, but it is equally easy to exaggerate the difficulties that individual terrorist movements and extremists now face in*

using such technologies. There is a clear need to examine how states can use such weapons covertly or through proxies, and forecast how widely spread each of these threats is likely to become in the future.

We need to reexamine the problem of vulnerability. We cannot hope to accurate predict our attacker or their means of attack, but we can do much to improve our analysis of vulnerability and shape our intelligence and planning effort around the need to detect threats to our greatest vulnerabilities. To be specific, there are several areas of vulnerability that need special attention:

- We need to conduct and systematically update our analysis of the vulnerability of our critical infrastructure, including financial systems, information systems, communications systems, utilities, and transportation nets and make sure our intelligence can focus on potential threats.
- We need to reexamine our vulnerability to the chemical threat in the light of fourth generation weapons, and the growing ease with which states, extremists, and terrorists can obtain them.
- We need to rethink the risk of biological attack: We need to look beyond the risk of the limited use of crude, long-known weapons and toxins, and assess the extent to which genetic weapons are increasing our vulnerabilities. We also need to look beyond single agent non-infectious attacks on human beings, and consider multiple agent attacks, infectious attacks, and/or attacks on our agriculture.
- We need to reconsider the cumulative risk of covert or terrorist nuclear attack: It still seems unlikely that any state or terrorist movement could both acquire a nuclear device in the near future, and be willing to take the risk of using it. The cumulative risk over time, however, is sufficiently great to justify more analysis of our key vulnerabilities.

It is important to note that the US intelligence community and Department of Defense is already addressing many of these issues, as is the National Security Council and a broader federal Homeland defense effort. At the same time, these are all areas where Congressional oversight can play a major role in assessing the quality of the intelligence effort and the broader effort within the Executive Branch.

OTHER PROBLEMS IN INTELLIGENCE

Let me close with several comments focused on the problem of intelligence coverage of terrorism and asymmetric warfare. It has been some years since I was directly involved in intelligence planning and assessment, but there are some things that never seem to change:

- *It is far easier to call for strategic warning than to get it, or get policymakers to,* act on it of they do receive it. We can always improve our analysis of warning indicators. In fact, the intelligence community does this all the time. We cannot, however, count on any method of analysis sorting through the constant "noise level" in these indicators and providing reliable probability analysis or warning. Furthermore, we cannot count on policymakers reacting.
- We should improve our analysis, but no system of warning, defense, and response can rely on strategic warning. Moreover, it is my impression that even when the intelligence community does make improvements, decision-makers choose to ignore unpopular or expensive warning or demand that the community free them from the burden of ambiguity and uncertainty.
- It is always easy for decision-makers to demand prophecy and attack intelligence analysis when they don't get it. This may explain why there are so many calls for improved strategic warning and so few calls for improved decision-maker response.
- *It is far easier to call for better HUMINT than it is to get it.* I have listened to three decades of calls for improved human intelligence. In practice, however, it remains as underfunded as ever, and partly because it is so difficult to make cost-effective investments and to be sure they pay off. Far too often, successes are matters of chance and not of the scale of effort.
- Yes, we should improve HUMINT—where we can show there is a feasible plan and a cost-effective path for success. However, calling for improved HUMINT all too often is both a confession of the severe limits of National Technical Means and a substitute for serious planning and effort.
- *New intelligence toys are not new systems, and systems always have limitations.* The other side of this coin is that we probably face growing limitations in our imagery and signals intelligence capabilities in many of the areas that affect our vulnerability to asymmetric warfare and terrorism. These are not a problem that should be addressed in open testimony, nor can I claim that my background in these issues is up-to-date. However, it is far from clear that some of

the extremely expensive improvements we plan in National Technical Means will really pay off in the areas we are discussing today, or that some of the new tactical detectors and sensors being developed are integrated into effective systems. There may well be a need for independent net intelligence assessment of our probable future capabilities in these areas.

- *We need more focus on weaponization, weapons effects, and different kinds of vulnerability.* Proliferation and changes in information warfare are creating major new challenges in how the community should assess the weapons available to state and extremist actors. This is particularly true of biotechnology and information warfare, but it also involves the risk of "dirty," unsafe, and unpredictable nuclear weapons. Most weapons effects analysis is badly dated, and related to use against military targets. Weaponization analysis often does not address the acute uncertainty that may occur in weapons effects, and most vulnerability analysis is now dated. The technical issues of what attackers can , really do, the problem intelligence may face in characterizing their resources, and the risk of combinations of new methods of attack—combining information systems and CBRN attacks, cocktails of biological weapons, etc. needs more attention.
- *We need an effective bridge between foreign intelligence and law enforcement that responds to the scale of the emergency.* We now have a wide range of barriers between foreign intelligence collection, surveillance of US citizens and activities within the US, military operations, and law enforcement activities. In general, these involve useful and necessary protections of American civil liberties. If, however, the threat rises to the level of a tangible risk an attack may use effective biological weapons, use nuclear weapons, or cripple our critical infrastructure, we need some way to react to a true national emergency that eliminates as many of these barriers as possible, and which does so at the state and local level and not just the federal one. We have long talked about the need for the "fusion" of intelligence and operations in warfighting. We may well face a similar need in Homeland defense, and the "fusion" of foreign intelligence and law enforcement activity will be critical.

One final point. Whenever new threats emerge, there is a natural tendency to call for new organizations, czars, and interagency structures. It is far easier to say that a new organization is needed than to get into the nitty gritty of actually having to improve existing capabilities or develop new ones. A set of problems involving this many uncertainties and new skills may or may not require new federal organizations, and new organizations within the intelligence community,

Ultimately, however, what improving our capability to deal with terrorism and asymmetric warfare requires most is resources and improving collection, analysis, and fusion at sophisticated technical levels. The real issue is one of how to improve depth, give the community the right perspective, and how to improve "quality," and not how to change organization or leadership. This requires both serious planning and a serious program and supporting budget. Changing the name on the door is almost mindlessly easy, but changing the capability within is what counts.

Chairman KYL. Thank you very much.

Dr. Alexander?

STATEMENT OF YONAH ALEXANDER, SENIOR FELLOW AND DIRECTOR, INTERNATIONAL CENTER FOR TERRORISM STUDIES, POTOMAC INSTITUTE FOR POLICY STUDIES, ARLINGTON, VIRGINIA

Mr. ALEXANDER. Thank you, Mr. Chairman. I appreciate the opportunity to appear today before this subcommittee. My only regret is that I don't have a written paper because I was out of town. But with your permission, I would like to submit a formal paper at a later date.

Chairman KYL. Absolutely.

Mr. ALEXANDER. In addition to that, I would like to mention that as an academician who works at a think tank and at a university center for terrorism studies, we have a great deal of publications that we would like to report to you about and to share with your staff, such as the new publication on Bin Ladin, on cyber terrorism, on super-terrorism, American perspectives, and so on and so forth.

If we may submit them to your staff, we would certainly appreciate that.

My intention basically is to make some preliminary remarks related to the threat and response. I fully agree with Tony Cordesman on some of the points he made because I think, No. 1, we have to learn lessons at history and look specifically at the nature of the threat. Now, we are discussing super-terrorism, biological, chemical, nuclear, cyber, but I would like to submit that even a very primitive kind of terrorism works and it is attractive, it is effective, and achieves a number of results.

We can go all the way back to the first century or to the 11th and 12th centuries, the Middle East, when they used primitive methods, but they were able to intimidate the Crusaders, for example, in the Middle East. So I think there are some lessons from history that we can take into account.

If we look at the situation today, obviously when we talk about contemporary terrorism, we talk about the new scale of violence both in terms of threats and responses. We are discussing the internationalization and brutalization of modern terrorism which actually is developing a new age of terrorism and super-terrorism with very serious implications for national, regional, and global security concerns.

I would like to underscore specifically about five dangers that we have to take into account. One danger is to the safety and welfare and rights of ordinary people. The second danger is to the stability of the state system the way we know it. The third is to the health of economic development. The fourth is to the expansion of democracy, and the fifth perhaps to the survival of civilization. By that I mean the worst is yet to come; it is not if, but when. Therefore, ensuring the safety of the citizens at home and abroad will continue to be every government's paramount responsibility in the coming years.

If I may look at the calendar of history, I would like to remind the Chairman and members of the Subcommittee that 30 years ago there was a bombing right here in the U.S. Senate perpetrated by the Weather Underground. And then 13 years ago, in Iraq, we found that the Iraqis used chemical weapons against the Kurds. And 6 years ago, we had a glimpse of the future when the Aum Shinrikyo used sarin gas in Tokyo.

Now, in 1995 I had the privilege, with my colleague Dr. Ray Klein from the Center for Strategic and International Studies, to prepare a study on state-sponsored terrorism for the Subcommittee on Security and Terrorism, chaired by Senator Jeremiah Denton. The question arises, what is new, and if you look at the situation in those days and the situation today, of course, at that time the Soviet Union perpetrated terrorism. Today, the Soviet Union is a victim of terrorism, as we have seen in the past few days.

Nevertheless, I think we cannot dismiss state-sponsored terrorism in the coming months and years. Although there is a study of the CIA for the year 2015 indicating that the involvement of states is going to be reduced, nevertheless we have to take into account some states that can be labeled as failure states or states that are being exploited by the terrorists.

So therefore what I am really suggesting is that we have to look at both state-sponsored terrorism and sub-state terrorism, the freelancers, those who are able to initiate terrorism at a very low cost and cause a great deal of damage to our society. Therefore, I think the international community, and particularly under the leadership of the United States, must take whatever steps are necessary in order to reduce the risks.

Again, it is not a question of recommendations of committees and commissions. I know that some of us were involved over the years working with some of these groups. Nothing is wrong with specific recommendations. The problem is really implementation of the recommendations, and we have to move step by step, not dramatically or drastically change the system.

Therefore, I think every segment of the community can play a role, not only the Government, not only Congress, but the community in general. And I refer to the media, I refer to religious organizations, to the educational structure, and so forth, and together I think we can defeat the terrorists and secure our value system.

I will stop here and be open to questions.

Chairman KYL. Thank you very much.

Both of you have commented on the need to concern ourselves with cyber attacks, and that seems to me to be a somewhat overlooked potential threat because it is not just against the Government, it is not just against our defense and national security capabilities, but also against the society at large, which then also has a spillover effect against national security.

What, in your view, should the U.S. Congress be doing to enhance our ability to deal with this problem of cyber attack, especially if we are to, as you say, Dr. Cordesman, size it to the state-sponsored terrorism threat, because clearly that would be the ultimate degree of cyber attack even though it might be coming from some group far smaller than state-sponsored? What could the Congress do to help begin to prepare us to deal with this threat?

I will start with you, Dr. Cordesman, and then Dr. Alexander.

Mr. CORDESMAN. Let me give one example. In the previous administration, John Hamre issued a directive in the Department of Defense that no critical system be hooked up to the Internet. One of the problems is that we right now are spending most of our critical infrastructure protection money trying to protect the software and entry into the systems, not to create systems which close out outside attack because they are truly critical. We, in general, do not have adequate standards.

It has become clear, for example, that within the Federal Government no department as yet can police itself. To the extent there have been successful audits of cyber defense, they have been done by the General Accounting Office. And the moment the General Accounting Office does not repeat the audit, the department generally goes back to failing to protect its systems.

But more than that, you do not see an effort to reduce vulnerability, to ensure that you can reconstitute the system rapidly, that if there is a really major and successful attack, there is some alternative. Now, this I suspect is going to require legislation and regulation. Departments are not going to spend money that is not ap-

propriated and they are not going to perform functions with money that is appropriated unless they are required to.

But the issue, I think, is broader than that. We can't provide any kind of warning or leak-proof system in cyber defense, and that means that critical industrial systems also have to be designed so that their vulnerability is limited, rather than trying to create firewalls or infinite layers of defense. There have to be backups. There have to be real tradeoffs where people understand that there is a liability for failing to protect these systems.

At present, it is just the reverse. All of the market forces say that you do the absolute minimum here because there is no reward. You are not going to get more profit. Nobody is going to congratulate you until you come under attack, if then. Even insurance companies really are not regulated to require effective cyber protection or effective standards be met.

Now, I hate to say that in any area the solution may be better law and better regulation, but here it is very difficult to see what market forces lead companies to prepare themselves unless there is a requirement that this be one of the rules of business.

Chairman KYL. So I take from that three basic recommendations: greater development of separate systems which are not tied to the Internet, a regulatory environment in which insurance would drive the hardening of these sites, and an ability to reconstitute systems immediately, with perhaps some Federal legislation and appropriate to achieve that.

Mr. CORDESMAN. Senator, I would add one more. I think it is absolutely critical that you honestly assess vulnerability. In a lot of cases today, people confuse the noise level of cyber attack with something serious, or the fact that cyber crime has replaced conventional crime is somehow seen as if this was a national threat. ell, criminals will always be with us, systems will always fail, and teenagers will always be teenagers.

We have not sorted out real vulnerabilities from the noise level of technological change. A good example is what happens every time there is a new virus. Somebody costs it several hundred million dollars, and this gets into the papers and everybody repeats the figure. But virtually all the time, when you really look at it, there was almost no economic cost; people did business the next day. This gross exaggeration of low-level threats and indifference to the issue as serious information warfare is as much of the problem.

Chairman KYL. Thank you.

Dr. Alexander?

Mr. ALEXANDER. I think fundamentally it is really the question of perception of the threat, because here we are talking about the blessing of the Internet to connect the entire world. On the other hand, unfortunately, it is also a curse, as we know, used by terrorists as propaganda and psychological warfare. It is used to communicate messages and to train people how to make bombs—in fact, one doesn't need to go to a training camp because he can get all the information on the Internet—and then for operational missions, as we have seen time and again.

Now, the question is really now can you strike a balance between the security concerns and civil liberties. I think this is a very im-

portant issue, and therefore there is a need not only for Government—we are talking about the role of Congress or the role of the Pentagon to stop the penetrations, and so on and so forth—I would like to submit that this is really a partnership of the Government and industry and academics and the public in general, because each segment of the community has a stake in this particular issue.

Again, it comes back to the question of perception because the American people today, I think, are confused about what is terrorism. Is it a criminal act? Is it low-intensity conflict? Is it an asymmetrical threat? Is it all-out war? If it is war, there are certain legal consequences, and people would be willing to forgo some civil liberties if the United States is at war.

So I think the first step is to put our act together in terms of a coherent definition of what terrorism is and to communicate that definition to the American public, to our friends, allies and adversaries, so there should be no mistake about where the United States stands on terrorism, and then to deal with the different kinds of threats—the biological, the chemical, the nuclear, the super. In fact, terrorists are today discussing even space terrorism. Looking ahead, what can they do in order to exploit space.

Therefore, I think we have to deal not only with the technology, but with the psychology and the mind set.

Chairman KYL. While Senator Feinstein is catching her breath here, let me just pursue this line of questioning and then we will join in together, if that is all right.

Let me get a little bit more specific, Dr. Cordesman, about your recommendation regarding insurance. It has seemed to me that while the U.S. Government could require that certain systems be separate and totally apart from the Internet—and, in fact, some are, and we could encourage perhaps some in academia or the private sector to develop systems that are similarly unconnected to the Internet and therefore far less vulnerable—that there is a great deal of commercial or industrial or non-governmental activity that nevertheless affects the Government.

Our transportation grid, our communications system, the energy grid, the financial systems—all of those things are interconnected for commercial reasons, and I too have been concerned about the lack of robustness to these. I had thought that perhaps losses occasioned by cyber attacks would result in liability determinations. The evolution of the law would create the rules. Insurance would provide the enforcement of those rules—insurance and, of course, legal decisions—and that would force the robustness.

I am not sure, however, that it would necessarily protect against the loss to Government, the loss of capability that would impact on our National security from a governmental point of view.

How do you see this evolution, and is this the area in which you see some role for governmental regulation?

Mr. CORDESMAN. Well, Senator, let me first address the word "Internet." It is very popular, it is a wonderful toy, and it actually has a great deal of substantive use. But the fact is most critical systems shouldn't be on the Internet; useful systems should be. And if useful systems are reconstituted three or 4 days later, it

really doesn't matter very much. Nobody dies, the economy doesn't fail.

So I think we have to make a clear distinction between those systems and systems, for example, like the functioning of the stock market or, as you mentioned, control of air traffic or major water systems or utility grids, most of which frankly should be off the Internet in any case.

Now, liability is an issue, but I think waiting for liability to happen is the kind of process that says you go into court after the problem has already occurred. So I would suggest a very narrow focus. I don't think that we need to regulate the Internet. What we need to do is to identify and regulate a very narrow range of critical systems, and the answer may not be the same in each case.

Sometimes it can be liability, sometimes it will have to be redundancy. In some cases, it will be systems which degrade gracefully and have backup. But we really don't have an ordered, structured approach to that problem either within the Government or within American industry, or for that matter on a global economic basis yet. And I think we have to begin by analyzing what is critical to protect and then find the measure tailored to the system rather than having one solution that fits all problems.

Chairman KYL. I appreciate that response.

Mr. Alexander, anything else on that point?

Mr. ALEXANDER. Well, just a footnote. I would say that this is one area where I think international cooperation is feasible because it affects everyone, and therefore we have to start step by step. I know some countries are trying to develop all kinds of structures to deal with the protection of sensitive information, for example, and so on. So it is not just a question of the United States; it is a regional problem and a global problem. And I think this is one way that I think we can get consensus.

Chairman KYL. Thank you very much.

Senator Feinstein has joined us and I will call on her now to make any kind of statement she would like to make or jump right in with the questioning of our second panel.

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. Thanks, Mr. Chairman, very much for holding the hearing. I think I will just put my statement in the record, if I may, and ask these questions.

It is my understanding from what I have seen that our Government has not clearly designated who would be in charge in responding to a terrorist incident. In a recent GAO report on counterterrorism policy in Canada, France, Germany, Israel, the UK, and the U.S., the United States was the only one of these countries that lacked a clear chain of command in response to a terrorist incident.

Are you concerned about this, and what should that chain of command, in your view, be?

Mr. CORDESMAN. If I may begin, Senator, I think in theory there is a chain of command. The problem is that it is too complex. We have a division—

Senator FEINSTEIN. Did you say it is too complex?

Mr. CORDESMAN. That is right. I mean, basically speaking, first if it is a low-level incident, to be perfectly honest, we have so many natural catastrophes and accidents that it isn't a stress on the system. But if we get a really large-scale terrorist attack that produces mass casualties, then all of a sudden the FBI and FEMA are confronted, as Dr. Alexander mentioned, with an effect close to war.

What happens then? Well, the system is simply not capable of responding at some central point to the complexity of the individual case. We have all kinds of lines of responsibility, but they won't work on a clear or timely basis.

The separation between FEMA, which is understaffed, underfunded and not equipped to deal with the effects of large-scale terrorism because it focuses on civil disasters—it simply is not ready. The FBI confronts the problems of foreign intelligence and State and local law enforcement, and let me note that the gaps there are as great as they are between the CIA and the FBI. It goes to the NSC, where the question of who is operational has to almost be improvised. If it is a really serious incident, the President has to be brought in.

You mentioned response. One problem we have never really addressed is what happens if it is a biological incident, because the actual responders particularly to multiple incidents or more than one agent are all tailored to medical services and biological response. If it is high-explosive, it may be the National Guard that would be the proper group. If it is nuclear, biological experts are not the people who would have to deal with that case.

We really have looked at this in Washington only from the top. We haven't looked at the consequences of different major acts of terrorism and how the chain of command and response would have to adapt.

Let me just give you one simple example. In most places in the United States, in the winter, most hospital beds are occupied. Many hospitals are in urban areas. If you have a biological attack, not only do you immediately cause a total saturation of local and regional health care, but basically the attack often will cover the area where the care is supposed to be provided.

Now, the Federal response to that is going to be to fly in emergency help to people who are, in general, supposed to meet that help at the airport. When it is FEMA or the FBI or some czar that is some czar that is in charge isn't going to help if that is the scenario.

Senator FEINSTEIN. From your study—let's say a building is blown up or a bus is blown up—who in the United States is immediately in charge of that incident, the top person?

Mr. CORDESMAN. Well, the top person will be almost invariably, unless it is on a Federal facility, the mayor or the head of the local jurisdiction who will be responsible for coordinating local law enforcement, which will treat it as a criminal act, and for coordinating the emergency response.

If it is on a Federal facility, for example, a military base, it would be the base commander. There will be all kinds of legal complications and they are going to spread out along with the response issues. If it is something like a water supply, however, which cuts

across, say, State or jurisdictional boundaries, then the issue would be whoever is in charge of the individual utility or facility.

But ultimately the first response always is local, and in the real world the authority level or chain of authority is local until Federal intervention or State intervention is required.

Senator FEINSTEIN. Well, let me respond. Having served as a mayor for 9 years in a form of government where the mayor was essentially in charge of the police department and the fire department and had the ability to ask for mutual aid, I am not sure as we go into more sophisticated types of terrorism that really having a mayor in charge is the best idea.

It seems to me, once an attack happens whatever the scale, immediately the Federal Government has some responsibility and there should be somebody there from the Federal Government with respect to protecting the chain of evidence, and also doing whatever is necessary to aid in protection of the people. I don't think you can leave the response to sophisticated international terrorism in the hands of a mayor. We had talked before about having a response team that could go into an area.

What would your recommendations be, Dr. Cordesman and Dr. Alexander?

Mr. CORDESMAN. Everything depends on the size and nature of the incident. That ones that you mentioned initially are sort of conventional terrorism. Indeed, in the Federal Government planning tends to be for incidents where there are less than 1,000 casualties because that is assumed to be the maximum worst case for practical planning. If it is biological or nuclear, of course, the attacks will be far larger.

The moment that this extends beyond a localized single event, the moment it involves a weapon of mass destruction, you must be able to bring in Federal authority and law enforcement and certainly FEMA immediately. At any level involving, I would think, frankly, a nuclear event or a major biological event, I don't believe that the Congress will ever properly fund FEMA to respond and you will be forced to bring in the Department of Defense.

That means that there must be somebody coordinating a tailored Federal response, and they have to begin hopefully within minutes of the ability to characterize the attack. Now, long before then, if it is international terrorism, one would have hoped that the kinds of issues discussed earlier, the cooperation between the CIA and FBI, would have improved to reduce the risk of incident.

Senator FEINSTEIN. Well, supposing the gentleman that tried to come across the Canadian border a couple of weeks before New Year's Eve 1999 was actually able to blow up something significant in Seattle, Washington, you are saying that that should be left up to the mayor to handle?

Mr. CORDESMAN. No, I am not saying it should be left up to the mayor. You asked what the chain of responsibility was, and in practice the FBI would come in later. Now, the FBI would not have here a jurisdictional problem because it is clearly a foreign terrorist. It might take time to establish that.

Depending on how the local jurisdiction handled the issue, you might get immediate, smooth cooperation between State, local, and Federal law enforcement. That is what I think would happen in

any major case. But as you know, there are sometimes communities where that relationship does not always work out as it should.

I would hope that the immediate action for any foreign terrorism would be what is called for under law because the FBI does have jurisdiction over acts of terrorism if they are defined as such, an issue which Dr. Alexander raised. Similarly, FEMA would have responsibility to assist State and local authorities immediately at the Federal level, depending on the size of the incident. But the critical issue you have raised is the size of the incident and what happens when local capabilities break down.

Senator FEINSTEIN. I just think in reality, having been there during a riot, it is very difficult. I happen to believe there ought to be someone in the Federal Government, that once a mayor presses a button or makes a phone call and expresses what kind of an attack it is, can immediately bring onto the scene whatever Federal reinforcements are available or helpful.

The White Night riot, when the assassin of my predecessor as mayor and another supervisor was just given a very brief sentence and there was an explosion in the city and police cars were being blown up and buildings were being attacked with rocks, was a very difficult situation. It took a long time to get everybody together, and then finally I called the Governor to exercise mutual aid. It all takes time before you know exactly what you have.

We became much more sophisticated about it after that, training police, how they work, all the details of it. But it is a little bit of a lesson to me that if you have, let's say, the Federal building blown up right next to city hall, you are into something entirely different and mutual aid isn't going to help very much. You are going to need immediate reinforcement. It may be military, it may be FBI. Some of it may be FEMA, but someone has got to make that decision, and make it quickly.

I am coming to believe that there ought to be someone on a Federal level that a local jurisdiction is able to consult with immediately, 24 hours day, that is helpful in making the decisions as to who is alerted, who is brought in, what the time line is. I think that would become particularly more important in a biological or a chemical reaction.

Mr. Alexander, would you like to comment?

Mr. ALEXANDER. Yes. Again, it comes, Senator, to the question of perception. Because the United States fortunately was not as victimized as some of the other countries that you mentioned, usually terrorism was looked upon as an irritant, a nuisance, something that will go away, very cyclical. So the culture was not there in terms of the concern of the people.

Today, the situation is changing. As Senator Kyl mentioned, the United States is really target No. 1 abroad and we have had terrible tragedies in Oklahoma and elsewhere. So I think the American people are much more sensitive to the issue of terrorism, and if the public would try to get involved and cooperate with Congress on what is needed, what kinds of tools are necessary to deal with the problem in terms of policies, in terms of organizational structure, in terms of upgrading intelligence and strengthening law enforcement, for example, perhaps, Senator Feinstein, as mayor this

wouldn't be your role to deal with a bioattack. Sometimes, you have to wait a couple of days before you know you are really under attack.

Therefore, I think what this Subcommittee is doing and other committees in Congress is extremely useful. As you know, there are probably 80 Federal agencies involved in different aspects of terrorism, and therefore certainly it is like an orchestra without a conductor. I think something has to be done to coordinate many of these activities. Some work, some don't, and therefore I think we have to monitor the operations very, very closely. First, we must assess the nature of the threat in order to know what kinds of responses are really suitable at home and abroad.

Senator FEINSTEIN. If you are really going to look at this as a practical application, every mayor, at least in California, has different authorities. Some city councils rotate a city council person as mayor every year. Some are strong mayors, and some are very weak mayors who just don't have the control. Some frankly don't have the ability to cope with a terrorist incident. I think in this country we are wide open to chaos without the ability to really have somebody who is able to send out an immediate assessment team, make the assessment, and set into motion a chain of events.

I am truly of the view, Mr. Chairman, that we really ought to write a big bill, a real reorganization of counterterrorism policy. We have been doing this now for 3 years, and we listen to report after report after report, all of which suggest that we are really unprepared. Even when we had our classified briefing a while ago, I didn't come out with a great sense of confidence that we were ready to respond to a terrorist event.

It seems to me that there is a recommendation somewhere in this, and I can't remember where it is but I thought it made sense, and that is that each President really ought to come forward with a plan as to how the administration would approach this in terms of a chain of command, an instant response, emergency provisions, investigative needs, and military precautions. It might be something that we could request the administration to do.

Chairman KYL. I might just note that just before you arrived, Dr. Cordesman made the point that while planning is certainly necessary, the tendency might be for yet one more planning document, one more reorganization, all of which reshuffles the chairs on the deck. That is my analogy, not his, but it adds very little value to the response.

I was going to follow up with a question that ties in directly with what you were just saying. Basically, what you want is a 911 for any kind of help that might be out there that the local group isn't immediately able to provide. If it is clearly a law enforcement kind of an attack and a conventional explosive blows up a building, the law enforcement people are going to be on the spot and they are going to be the ones who take charge. If, all of a sudden, everybody within a 10-block area is getting really sick from something, the health care people are going to come in and figure out that there is some kind of a problem.

But in either event, if there is a 911 number at the Federal level that people can call to get whatever kind of help might be available and a general plan at the Federal level, it seems to me that that

is one way of providing whatever kind of help might be available in a fairly efficient way. But I too would be skeptical of focusing our attention too much on reorganization, strategy documents, and the like. I am really interested in getting beyond that to the value-added components of dealing with terrorism as well.

A response from either one of you to that comment would be appreciated.

Mr. CORDESMAN. Let me give you, I think, a tangible example. Congress legislated that there be a document provided by OMB describing the programs that are currently underway. As far as I know, I have not talked to anybody who has held hearings on what we are actually spending the money on. It is $11.7 billion in the last fiscal year; $1.5 billion of it is dedicated to deal with the effects of weapons of mass destruction. It is spread out among 17 different groups.

On paper, Senator, for example, there is a Biological Response Team. The problem is it may have 17 people and 2 doctors in it, and I am not sure that is going to help any city on the West or East Coast in the event of a biological incident.

I think that when you talk about organization, it is very important to have one person in charge, and there have been proposals putting it in the Office of the Vice President, having a Cabinet-level official, having someone on the order of the drug czar, putting the response elements in FEMA, and strengthening coordination within the FBI. I don't know which of these the President would prefer, but it is clear that you not only need someone to call, but somebody who can do something in response.

My suggestion to you would be that the kind of examination which is already being made of where the Federal money is going needs very careful examination to see what really needs to be fixed. It is fairly obvious, looking at the numbers, that right now virtually all the money we spend is on improving Federal buildings and their resistance to high explosives. That is the one threat on which about $7 billion of the money has been going.

I think as you look into this you are going to find there is no long-term planning. Agencies improvise and compete from year to year. In program after program, they don't know what they would have to spend to develop a real capability. Technologies are being funded, but nobody knows what system they would go into if they worked, whether they would really deal with the threat of future technology, or what they would cost to deploy and whether it would be a State, local, or Federal deployment that would be required.

So we have one organizational study after another trying to figure out who it is that answers the telephone, but no review of Congress' traditional function, which is to look at where the money is really going and whether it is being spent to a purpose.

Senator FEINSTEIN. I have been brought up to believe that the primary role of government is to protect the people, and I really believe that. If I am mayor and something blows up, I want to maximize every resource I have as fast as I possibly can.

I really agree with you, Dr. Cordesman. I think that domestic terrorism is something that is very appropriate to be part of the portfolio of either a Vice President or a Cabinet member. When a building has just blown up and the suspicions are that it is terror-

ism, I can pick up the phone and say we have got a major incident on our hands, we need help, we need it right now. I want a team that can come out and take a look at this situation, and also help us with A, B, C, D, and E.

Californians pay more than $20 billion in taxes a year that they don't get back in services. It is not too much to ask that the Federal Government be able to provide counterterrorism assistance. Terrorism is increasing in this world, and we ought to be prepared for it. And to be prepared for it means that certain people have to be accountable to do certain things.

I have been looking at this for 3 years. It is still unclear to me of who is really in charge of what, or where as a mayor I would go to get help. That is not clear; it is not clear out there anywhere in the United States. I think the time has come for us to try and make that clear to people.

End of speech.

Mr. ALEXANDER. May I just make another footnote here? I fully agree with you. I wanted to call you mayor, Senator, in terms of your experience, and this is life. I mean, someone has to be on the front line and be able to save lives and minimize the threat.

But I would like to submit to you that we have to see it in a broader perspective, not only in terms of what is happening in the United States but what is happening abroad. Particularly, I am talking about Americans and American citizens who are all over the world, as we know, about 10 million of them at a time, and they need protection as well; of course, the military or the diplomats, and we have seen that.

My concern is that we are not putting that together in terms of also the international protection. And recalling the tragedies that American servicemen went through for so many years, and I have seen some firsthand, I believe that we have to learn the lessons of the past; that is to say, the State Department after the attacks on the embassies in Kenya and Tanzania immediately tried to figure out what could they do to protect members of the State Department. So they instituted some measures both at the State Department right here in Washington as well as at embassies abroad. Then they started training against weapons of mass destruction, and so forth.

But that particular action did not prevent the terrorists from attacking the U.S. Destroyer Cole and killing Americans on the ship. And this really means that there is a need somehow, No. 1, to strengthen the intelligence capability, the quality, in terms of human and technological to deal with future threats to Americans abroad, and also to work with like-minded nations to coordinate the activities.

For example, Tony mentioned emergency medical preparedness. Not only in the United States are there not enough beds, but when we talk about the situation abroad and how to save those who are injured, if it takes about 12 hours to get some assistance, then it is too late.

So what I am really suggesting is, Senator, that we have to see it as a comprehensive threat to the United States. It is not a nuisance, it is not an irritant. It is a national security threat, and therefore I think we have to mobilize all the capabilities and to

look at the recommendations—some of them are really excellent—in terms of responsibility, in terms of organizational structure, and so on and so forth.

If we are not going to do it, especially the United States as a super-power, as the leader of the Free World, if I may use this term, I really believe that we have a special responsibility to provide the leadership.

Senator FEINSTEIN. Thank you very much.

Chairman KYL. Let me just close with this question, since you raised the issue, Dr. Alexander, and in his written testimony Dr. Cordesman makes the same point. Obviously, you would like to try to thwart the terrorist incident in the first instance. Intelligence is key to that capability, and while we have some success with signals intelligence, human intelligence is the primary source of information that enables us to thwart terrorist attacks.

Incidentally, for those in the audience who might be interested, we have had testimony each year for I think 3 years from the Director of the FBI that each year our intelligence agencies are able to thwart about a dozen major terrorist attacks through the use of good intelligence. These are very rarely made public. We know of the attacks that are successful, but we rarely hear about those that have been prevented through good intelligence and there are a number of them.

Dr. Cordesman, you specifically testified that human intelligence is underfunded and that it is critical to this effort. Why do you think it is so underfunded, and what can we do?

Since both of us also serve on the Intelligence Committee, even though that is not directly related to the Judiciary Committee, the intelligence-sharing questions do arise. In any event, we are all interested in the subject.

How can we better fund our human intelligence?

Mr. CORDESMAN. Well, I was saying to one of your staff, Senator, that several centuries ago I was the Director of Intelligence Assessment in the Office of the Secretary of Defense, and the Congress decided it would be a good idea to recommend an increase in human intelligence resources and 1 year later we were having RIFs.

In general, any time anybody in Congress seems to propose this—I am not sure there is a cause and effect relationship—the resources end up mysteriously being cut. So I have to be very careful about what I say here.

I think frankly you have, in general, a very effective intelligence community. We always underfund the human dimension and the analytic dimension, and we always tend to put lots of money into national technical means. I am not sure there are any savings to be made in national technical means, and it is not glamorous to say that you simply give people in the community more resources to plus-up the capabilities they already have. But I think that is part of the problem that everybody wants to reorganize or make it more efficient, but they don't want to spend more money in a focused way where it is really needed.

I think, too, you need to be very cautious because human intelligence, as you know, is often defined as collection; it is getting more sources overseas. Dr. Alexander mentioned the need for bet-

ter international cooperation. There is a need to put a lot more money into the analysis side, areas like data mining, areas which get around the unreliability of defectors and the inability to penetrate inside terrorist nets.

It takes a lot of time to develop a real expert on terrorism or on any given method of attack. And with new technologies like biological weapons and other methods, we tend to put people into growing sections in the community, but if they are not out or promoted in 3 years, it is a career killer, and that problem has been going on for decades.

So I think what you need to do is look in-depth at what is going on inside the intelligence community, figure out precisely what existing elements can be strengthened, and ensure that the money really goes to analysis in human intelligence and not to more managers or more coordination. In general, I believe the intelligence community is capable of greatly expanding its capabilities if somebody will be patient enough and realistic enough to give them the money they need.

Chairman KYL. I might add that as long as the intelligence funding is a percentage function of the Defense budget, there is an inherent arbitrary limitations on what can be devoted to intelligence-gathering.

Mr. ALEXANDER. If I may, Senator, I think that clearly is a very important issue. The other issue that I would like to suggest—and it was raised in some of the commission reports, the National Commission on Terrorism, Ambassador Bremer, and so forth—there are certain legal constraints on the capability of the agencies to function.

If we want them to do the job, we have to give them the tools to do it within the framework of law, of course. But if there are too many regulations and constraints even to recruit someone from a terrorist group to work with us—this is not someone would like to have dinner with, but nevertheless we need information and information can save lives. So really this is the question of the perception of the threat.

I would like to suggest that today, since we do have a trend of loose international networks like the Bin Ladin structure that can operate in some 55 countries around the world and mobilize people in order to strike against the United States, which is really target No. 1, the intelligence community, as we know, time and again is the first line of defense. And if they don't have the tools, it would be similar to taking away the tools from the police at the local level or the State level.

So therefore I think the American people have to consider the nature of the threat and, if the threat is really imminent, to do whatever is necessary, and particularly to support the intelligence community.

Chairman KYL. I thank you very much for those views. Obviously, some of these comments would perhaps do a little more good if they were heard by some of our other colleagues who aren't here. In Senator Feinstein and I, you have two people who are obviously committed to trying to get some help.

We will try to put together the three different reports that have been issued within the last 12 months or so, finding the common

areas for recommendations that we can at least agree upon, and without suggesting that all of this is legislative in nature, at least pull those things together that do require some legislative action and put it into a draft bill.

We would like to submit that to you for your review so you can give us your feedback on whether we are on the right track from your point of view, and then we are going to try to run that through the House and Senate this year. If you have any further recommendations for us, we would be happy to receive those, as I said at the outset of the hearing. Though we are not joined by a lot of our colleagues here today, we will share the information that we can summarize from this hearing with them in an effort to try to get their support as well.

I very much appreciate your testimony today, and look forward to your continued evaluation of our product and your advice as we move forward. Thank you very much.

This hearing is adjourned.

[Whereupon, at 3:50 p.m., the Subcommittee was adjourned.]