

COMBATING TERRORISM: A PROLIFERATION OF STRATEGIES

HEARING

BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS AND INTERNATIONAL
RELATIONS

OF THE

COMMITTEE ON
GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

MARCH 3, 2003

Serial No. 108-20

Printed for the use of the Committee on Government Reform



Available via the World Wide Web: <http://www.gpo.gov/congress/house>
<http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

87-702 PDF

WASHINGTON : 2003

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 GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana	HENRY A. WAXMAN, California
CHRISTOPHER SHAYS, Connecticut	TOM LANTOS, California
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
JOHN L. MICA, Florida	PAUL E. KANJORSKI, Pennsylvania
MARK E. SOUDER, Indiana	CAROLYN B. MALONEY, New York
STEVEN C. LATOURETTE, Ohio	ELIJAH E. CUMMINGS, Maryland
DOUG OSE, California	DENNIS J. KUCINICH, Ohio
RON LEWIS, Kentucky	DANNY K. DAVIS, Illinois
JO ANN DAVIS, Virginia	JOHN F. TIERNEY, Massachusetts
TODD RUSSELL PLATTS, Pennsylvania	WM. LACY CLAY, Missouri
CHRIS CANNON, Utah	DIANE E. WATSON, California
ADAM H. PUTNAM, Florida	STEPHEN F. LYNCH, Massachusetts
EDWARD L. SCHROCK, Virginia	CHRIS VAN HOLLEN, Maryland
JOHN J. DUNCAN, Jr., Tennessee	LINDA T. SANCHEZ, California
JOHN SULLIVAN, Oklahoma	C.A. "DUTCH" RUPPERSBERGER, Maryland
NATHAN DEAL, Georgia	ELEANOR HOLMES NORTON, District of Columbia
CANDICE S. MILLER, Michigan	JIM COOPER, Tennessee
TIM MURPHY, Pennsylvania	CHRIS BELL, Texas
MICHAEL R. TURNER, Ohio	
JOHN R. CARTER, Texas	BERNARD SANDERS, Vermont (Independent)
WILLIAM J. JANKLOW, South Dakota	
MARSHA BLACKBURN, Tennessee	

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL
RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

MICHAEL R. TURNER, Ohio	DENNIS J. KUCINICH, Ohio
DAN BURTON, Indiana	TOM LANTOS, California
STEVEN C. LATOURETTE, Ohio	BERNARD SANDERS, Vermont
RON LEWIS, Kentucky	STEPHEN F. LYNCH, Massachusetts
TODD RUSSELL PLATTS, Pennsylvania	CAROLYN B. MALONEY, New York
ADAM H. PUTNAM, Florida	LINDA T. SANCHEZ, California
EDWARD L. SCHROCK, Virginia	C.A. "DUTCH" RUPPERSBERGER, Maryland
JOHN J. DUNCAN, Jr., Tennessee	CHRIS BELL, Texas
TIM MURPHY, Pennsylvania	JOHN F. TIERNEY, Massachusetts
WILLIAM J. JANKLOW, South Dakota	

EX OFFICIO

TOM DAVIS, Virginia	HENRY A. WAXMAN, California
LAWRENCE J. HALLORAN, <i>Staff Director and Counsel</i>	
R. NICHOLAS PALARINO, <i>Senior Policy Advisor</i>	
THOMAS COSTA, <i>Professional Staff Member</i>	
ROBERT A. BRIGGS, <i>Clerk</i>	
DAVID RAPALLO, <i>Minority Counsel</i>	

CONTENTS

	Page
Hearing held on March 3, 2003	1
Statement of:	
Decker, Raymond, Director, Defense Capabilities and Management Team, U.S. General Accounting Office, accompanied by Stephen L. Caldwell, Assistant Director, U.S. General Accounting Office	12
Gilmore, James S., III, chairman, Advisory Panel to Assess the Domestic Response Capabilities for Terrorism Involving Weapons of Mass De- struction; Michael E. O'Hanlon, senior fellow, foreign policy studies, the Sydney Stein, Jr. Chair, the Brookings Institution; John Newhouse, senior fellow, Center for Defense Information; and Andrew F. Krepinevich, executive director, Center for Strategic and Budgetary Assessments	58
Letters, statements, etc., submitted for the record by:	
Decker, Raymond, Director, Defense Capabilities and Management Team, U.S. General Accounting Office, prepared statement of	15
Gilmore, James S., III, chairman, Advisory Panel to Assess the Domestic Response Capabilities for Terrorism Involving Weapons of Mass De- struction, prepared statement of	62
Krepinevich, Andrew F., executive director, Center for Strategic and Budgetary Assessments, prepared statement of	148
Kucinich, Hon. Dennis J., a Representative in Congress from the State of Ohio, prepared statement of	7
Newhouse, John, senior fellow, Center for Defense Information, prepared statement of	119
O'Hanlon, Michael E., senior fellow, foreign policy studies, the Sydney Stein, Jr. Chair, the Brookings Institution, prepared statement of	102
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	3

COMBATING TERRORISM: A PROLIFERATION OF STRATEGIES

MONDAY, MARCH 3, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING
THREATS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 1 p.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Turner, Murphy, Janklow, Kucinich, and Bell.

Staff present: Lawrence Halloran, staff director and counsel; R. Nicholas Palarino, Ph.D., senior policy advisor; Thomas Costa, professional staff member; Robert A. Briggs, clerk; Mackenzie Eaglen, fellow; David Rapallo, minority counsel; and Jean Gosa, minority assistant clerk.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats and International Relations hearing entitled, "Combating Terrorism: A Proliferation of Strategies," is called to order.

Almost 2 years before the attacks of September 11, 2001, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, far more widely and succinctly known as the Gilmore Commission, concluded the United States lacked a coherent, functional national strategy to guide disparate counterterrorism efforts. In testimony before the subcommittee on March 26, 2001, the Commission's vice chairman said, "a truly comprehensive national strategy will contain a high-level statement of national objectives coupled logically to a statement of the means used to achieve these objectives."

The Bush administration inherited a loose collection of Presidential directives and law enforcement planning documents used as a strategic framework, but that fragile construct collapsed with the World Trade Center on September 11th. The brutal nature of the terrorist threat shattered naive assumptions terrorists would be deterred by geographic, political, or moral borders.

A new strategic paradigm was needed. Containment, deterrence, reaction and mutually assured destruction no longer served to protect the fundamental security interest of the American people. The threat demands detection, prevention, and a proactive, preemptive approach to self-defense.

To meet the demands of a new, more dangerous world, the executive branch has promulgated strategy statements articulating national goals for various aspects of the war on terrorism. Subordinate to the overarching national security and military strategies, other plans guide efforts to secure the homeland, combat terrorism abroad, integrate military response capabilities, combat weapons of mass destruction, stanch terrorist funding, secure cyberspace and protect critical national infrastructure.

A strategy famine has given way to a variable feast of high-level statements of national objectives and tactics to defeat the multifaceted foe that is global terrorism. Today we ask how these strategies link to form the national comprehensive policy recommended by the Gilmore Commission. Are they dynamic to meet changing adaptable threats? Do they guide the application of finite resources to achieve critical objectives? And how do we know if they are working?

Just as reorganizing the Federal Government to counterterrorism will take time, reorienting the U.S. long-term strategic mindset will require sustained effort and hard choices. Some fundamental elements of a fully integrated preparedness and response strategy are not yet evident. State officials and local first responders are still waiting to know how much will be expected of them in the event of a major incident. What capabilities in terms of training and equipment should be resident at the local level? When and how should Federal capabilities be brought to bear?

To help us begin our consideration of these important questions today, we welcome two panels of distinguished witnesses, including former Governor James Gilmore, chairman of the advisory commission that has been and remains on the forefront of the national debate on combating terrorism. In future hearings, we will hear from administration representatives and others to address specific elements of the strategic bulwark against terrorism.

We welcome all our witnesses and look forward to their testimony. At this point, the Chair would recognize the distinguished gentleman, our ranking member, Mr. Kucinich.

[The prepared statement of Hon. Christopher Shays follows:]

TOM DAVIS, VIRGINIA
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

ONE HUNDRED EIGHTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

Henry (HSA) 225-6174
Henry (GCR) 225-6061

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
E-mail: hr_groc@mail.house.gov

Statement of Rep. Christopher Shays
March 3, 2003

Almost two years before the attacks of September 11, 2001, the *Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* – far more widely and succinctly known as the Gilmore Commission – concluded the United States lacked a coherent, functional national strategy to guide disparate counterterrorism efforts. In testimony before this Subcommittee on March 26, 2001, the Commission’s Vice Chairman said, “a truly comprehensive national strategy will contain a high-level statement of national objectives coupled logically to a statement of the means used to achieve these objectives.”

The Bush Administration inherited a loose collection of presidential directives and law enforcement planning documents used as a strategic framework. But that fragile construct collapsed with the World Trade Center on September 11th. The brutal nature of the terrorist threat shattered naïve assumptions terrorists would be deterred by geographic, political or moral borders.

A new strategic paradigm was needed. Containment, deterrence reaction and mutually assured destruction no longer served to protect the fundamental security interests of the American people. The threat demands detection, prevention and a more proactive, preemptive approach to self-defense.

To meet the demands of a new, more dangerous world, the executive branch has promulgated strategy statements articulating national goals for various aspects of the war on terrorism. Subordinate to the overarching national security and military strategies, other plans guide efforts to secure the homeland, combat terrorism abroad, integrate military response capabilities, combat weapons of mass destruction, staunch terrorist funding, secure cyberspace and protect critical national infrastructure.

A strategy famine has given way to a veritable feast of high-level statements of national objectives and tactics to defeat the multifaceted foe that is global terrorism. Today we ask how these strategies link to form the comprehensive national policy recommended by the Gilmore Commission. Are they dynamic enough to meet changing, adaptable threats? Do they guide the application of finite resources to achieve critical objectives? And, how will we know if they are working?

Just as reorganizing the federal government to counter terrorism will take time, reorienting the U.S. long-term strategic mindset will require sustained effort and hard choices. Some fundamental elements of a fully integrated preparedness and response strategy are not yet evident. State officials and local first responders are still waiting to know how much will be expected of them in the event of a major incident. What capabilities – in terms of training and equipment – should be resident at the local level? What and how should federal capabilities be brought to bear?

To help us begin our consideration of these important questions today, we welcome two panels of distinguished witnesses, including former Governor James Gilmore, chairman of the advisory commission that has been, and remains, on the forefront of the national debate on combating terrorism. In future hearings, we will hear from Administration representatives and others to address specific elements of the strategic bulwark against terrorism.

We welcome all our witnesses and look forward to their testimony.

Mr. KUCINICH. Thank you very much, Mr. Chairman. I would like to extend a warm welcome to you and everyone connected with the work of our committee and to let you know that I look forward to working with you in this session.

Mr. SHAYS. Likewise.

Mr. KUCINICH. As you know, Mr. Chairman, we worked together in the last Congress to conduct oversight over the administration's efforts to secure our country against terrorist attacks. After the awful events of September 11th, it became more evident than ever that we needed a rational approach to protecting the American people.

Officials from the U.S. General Accounting Office, who are appearing before us again today, testified that the No. 1 step in crafting a national strategy was a comprehensive threat and risk assessment. Before we reorganized ourselves or allocated additional funding, we needed to understand and to prioritize the true threats to our Nation.

Mr. Chairman, on October 15, 2001, you and I joined together and we were accompanied by our counterparts on the full committee, Chairman Burton and Ranking Member Waxman, and the four of us signed a letter to President Bush. We urged the President to conduct exactly this type of assessment. In the spirit of bipartisanship, we moved forward and asked the President to use the opportunity of Governor Ridge's appointment to carefully examine all the threats we face.

Unfortunately, President Bush was not responsive in regard to our request. He did not respond to the committee. The administration moved ahead with the new Department of Homeland Security and produced a new budget, all without taking the initial step of completing a comprehensive threat, risk, and vulnerability assessment.

What is the result of this? Today's hearing is aptly entitled, "A Proliferation of Strategies." The administration has been proliferating national security strategies, nearly a dozen by my count, without any logical or demonstrable sense of priorities.

This lack of logic and the lack of priorities is exemplified by the administration's push for a preemptive attack on Iraq. The administration has not been able to make any kind of a credible connection between Iraq and al Qaeda with regard to September 11th, nor has the administration produced credible evidence connecting Iraq and September 11th. Yet the administration is moving ahead with the preemptive war despite the fact that Iraq poses no imminent threat to the United States.

This rush to war, in the face of international opposition, threatens to alienate the United States from the international community at the very moment we need international cooperation to root out terror. By pushing our Nation and the world to the verge of a historic preemptive attack, we are making America far more dangerous as a place to live.

I would suggest that whatever strategies we are discussing here must take into account the impact of any preemptive action by the United States against Iraq, because it's quite likely that such action, according to reports I've heard, Mr. Chairman, from the FBI that were published in the New York Times, it's quite likely such

action could result in more terrorist attacks being directed against this country. So that's why it's important we have this hearing.

This weekend's capture of Khalid Sheik Mohammed, the suspected mastermind behind numerous al Qaeda attacks by Pakistan, the capture that was effected with the help of Pakistan, once again demonstrates the great importance of international coalitions and cooperation in our ongoing efforts to root out the terrorists. The administration's rush to a historic preemptive war against Iraq, I believe, threatens to isolate our country and alienate allies that we need in our efforts to disrupt, capture, and dismantle the al Qaeda network.

I thank the Chair.

Mr. SHAYS. I thank the gentleman.

[The prepared statement of Hon. Dennis J. Kucinich follows:]

**Opening Statement
Representative Dennis J. Kucinich**

**Ranking Member
Subcommittee on National Security,
Emerging Threats, and International Relations**

March 3, 2003

GOOD MORNING, MR. CHAIRMAN. I WOULD LIKE TO EXTEND A WARM WELCOME TO EVERYONE AS WE BEGIN THE SUBCOMMITTEE' S WORK FOR THE 108TH CONGRESS.

AS YOU KNOW, MR. CHAIRMAN, WE WORKED TOGETHER LAST CONGRESS TO CONDUCT OVERSIGHT OVER THE ADMINISTRATION' S EFFORTS TO SECURE THE COUNTRY AGAINST TERRORIST ATTACKS. AFTER THE HORRENDOUS EVENTS OF SEPTEMBER 11, IT BECAME MORE EVIDENT THAN EVER THAT WE NEEDED A RATIONAL APPROACH TO PROTECTING THE AMERICAN PEOPLE.

OFFICIALS FROM THE U.S. GENERAL ACCOUNTING OFFICE, WHO ARE APPEARING BEFORE US AGAIN TODAY, TESTIFIED THAT THE NUMBER ONE STEP IN CRAFTING A NATIONAL STRATEGY WAS A COMPREHENSIVE THREAT AND RISK ASSESSMENT. BEFORE WE REORGANIZED OURSELVES OR ALLOCATED ADDITIONAL FUNDING, WE NEEDED TO UNDERSTAND AND PRIORITIZE THE TRUE THREATS TO OUR NATION.

MR. CHAIRMAN, ON OCTOBER 15, 2001, YOU AND I JOINED TOGETHER, WITH OUR COUNTERPARTS ON THE FULL COMMITTEE, CHAIRMAN BURTON AND RANKING MEMBER WAXMAN, AND THE FOUR OF US SIGNED A LETTER TO

PRESIDENT BUSH URGING HIM TO CONDUCT EXACTLY THIS TYPE OF ASSESSMENT. WE PUT ASIDE PARTISANSHIP AND ASKED THE PRESIDENT TO USE THE OPPORTUNITY OF GOVERNOR RIDGE'S APPOINTMENT TO CAREFULLY EXAMINE ALL OF THE THREATS WE FACE.

UNFORTUNATELY, PRESIDENT BUSH IGNORED US. HE NEVER RESPONDED TO THE COMMITTEE, HE PUSHED AHEAD WITH THE NEW DEPARTMENT OF HOMELAND SECURITY, AND HE PRODUCED A NEW BUDGET — ALL WITHOUT TAKING THE INITIAL STEP OF COMPLETING A COMPREHENSIVE THREAT, RISK, AND VULNERABILITY ASSESSMENT.

NOW, WHAT IS THE RESULT OF THIS? TODAY'S HEARING IS APTLY ENTITLED "A PROLIFERATION OF STRATEGIES." THE BUSH ADMINISTRATION HAS BEEN CRANKING OUT NATIONAL STRATEGIES — NEARLY A DOZEN BY MY COUNT — WITHOUT ANY LOGICAL OR DEMONSTRABLE SENSE OF PRIORITIES.

THIS LACK OF LOGIC AND PRIORITIES IS EXEMPLIFIED BY THE BUSH ADMINISTRATION'S PUSH FOR A PREEMPTIVE ATTACK ON IRAQ. THE ADMINISTRATION CANNOT MAKE A CONNECTION BETWEEN IRAQ AND AL-QAEDA. NOR HAS THE ADMINISTRATION PRODUCED EVIDENCE CONNECTING IRAQ AND 9/11. YET, THE ADMINISTRATION IS BULLYING AND BUYING SUPPORT FOR A PREEMPTIVE WAR AGAINST IRAQ DESPITE THE FACT THAT IRAQ POSSES NO IMMINENT THREAT THE UNITED STATES.

THE ADMINISTRATION'S RUSH TO WAR, IN THE FACE OF INTERNATIONAL OPPOSITION, THREATENS TO ALIENATE THE UNITED STATES FROM THE INTERNATIONAL COMMUNITY AT THE VERY MOMENT WE NEED INTERNATIONAL COOPERATION TO ROOT OUT TERROR. BY PUSHING OUR NATION, AND THE WORLD, TO THE VERGE OF A HISTORIC PREEMPTIVE ATTACK, WE ARE MAKING THE AMERICA A FAR MORE DANGEROUS PLACE.

THIS WEEKEND'S ARREST OF KHALID SHAIKH MOHAMMED, THE SUSPECTED 'MASTERMIND' BEHIND NUMEROUS AL-QAEDA ATTACKS, BY PAKISTAN OVER THE WEEKEND ONCE AGAIN DEMONSTRATES THE GREAT IMPORTANCE OF INTERNATIONAL COALITIONS AND COOPERATION IN OUR ONGOING EFFORTS TO ROOT OUT TERRORISTS. THE ADMINISTRATION'S RUSH TO A HISTORIC PREEMPTIVE WAR AGAINST IRAQ THREATENS TO ISOLATE THE UNITED STATES AND ALIENATE THE VERY ALLIES THAT WE NEED IN OUR EFFORTS TO DISRUPT AND CAPTURE AL-QAEDA TERRORISTS.

Mr. SHAYS. At this time, the Chair would recognize Mr. Janklow, former Governor of South Dakota, and then we will recognize Mr. Murphy from Pennsylvania. This is our first hearing and we're delighted to welcome both of them. Mr. Janklow, you have the floor.

Mr. JANKLOW. Thank you, Mr. Chairman, very much. And I am going to be very brief in my comments.

As I had an opportunity to review the strategies that were put forth by staff, I believe there were eight in number, it becomes really clear as it's been suggested, that we have had a proliferation of strategies enunciated and, at the same time, they are inter-related in certain respects, overlapping in certain respects. What I think we do lack is one clear overall strategy.

Now that's really not surprising. Notwithstanding political comments any of us want to make, this President was President for 9 months when the World Trade Center was attacked and we were subjected to the greatest terrorist attack in the history of this country. As a matter of fact, I believe it was the War of 1812 the last time that America, in a substantive way, had enemy soldiers within our borders operating.

Be that as it may, this administration inherited no strategic plans at all; that occasionally cruise missiles would be launched against some site in Afghanistan at an empty camp to enunciate some kind of announcement. But other than that, there really wasn't any clear cohesive strategy. But the important thing is now we have thousands of dead people. We have enormous damage to individuals' lives, survivors' lives. We have trauma the likes of which this country has never known before. We have untold damage to our economy totaling in the hundreds of billions of dollars. And terrorists have figured out they have the ability to bring America virtually to a standstill.

Five or six anthrax letters stopped the U.S. Postal Service, and, for all practical purposes, most of the governments in America, from being able to function for a period of time. The airlines were shut down. America's economy, for all practical purposes, was shut down.

And so, Mr. Chairman, I look forward to your leadership and working with you and the other Members of the Congress, the administration, and the American people to do what we can to come up with an overall program, laying out the road map in a very clear—in very enunciated ways, specifically setting forth what it is that we are trying to accomplish and the objectives by which we mean to accomplish that.

I realize when I say that, it is not unlike a play book for a football game; that you go into the football game with a play book and by the time the second play is called, the other team intercepts your ball and your play book is back to the drawing board for modification.

But we in this country have about 18,000 law enforcement units that have never before had to work together in an absolutely coordinated way. In my State of South Dakota, which is one of the least populated in the Union and one of the largest—as I tell people in my congressional district, it is just slightly smaller than Great Britain in terms of size; we have 534 fire departments within the State of South Dakota, over 250 of which are in communities

of less than 1,000 people. So we can begin to understand the magnitude on a national scale of what it is that we have to deal with and how we have to address it.

So, Mr. Chairman, I am pleased that you have been selected to be our chairman, with respect to this subcommittee, and look forward to working with you and others as we move forward to try and get accomplishments done at the speed of light to better protect and secure the American people in this country.

Mr. SHAYS. Thank you very much.

At this time we will call on Mr. Murphy from Pennsylvania.

Mr. MURPHY. Thank you, Mr. Chairman. I first of all commend you for calling this hearing. It is very important that if there's anything that the Government Reform Committee should be doing during this time, it is looking at ways to reform our strategies on national security; to make them more efficient, both in local emergency services, as Congressman Janklow just alluded, but also at the State and national level. We have to be united in our message, united in our strategy, and then united in our means of implementing that strategy during a time when people will—and certainly the terrorists will look for ways to divide us. They are counting on our short memory of events, although they are burned in our memories forever. They are counting on Americans to be fickle about their memories and counting on us to be divisive in our politics as they watch the news, and they mistake freedom of speech for disunity.

There may be times when this committee and other committees may have people who do not agree, but I want them to also know a message that as we iron out ways of making these strategies more efficient, as we'll hear from testimony today, these are geared toward working in a united way to take care of these problems quickly and efficiently. So I look forward to the hearing, Mr. Chairman. Thank you.

Mr. SHAYS. I thank the gentleman.

We will call our first panel. Our panel is Mr. Raymond Decker, Director, Defense Capabilities and Management Team, U.S. General Accounting Office, accompanied by Stephen Caldwell, Assistant Director of Defense Capabilities and Management. As is our practice, we will ask you gentlemen to stand and we will swear you in.

[Witnesses sworn.]

Mr. SHAYS. I thank the gentlemen. Note for the record that our witnesses have responded in the affirmative. I think we only have one statement. That's from you Mr. Decker, correct?

Mr. DECKER. That's correct.

Mr. SHAYS. And just let the record note, Mr. Decker, we have worked with you for many years and we appreciate very sincerely the work of the GAO and specifically your work. Thank you very much. And, Mr. Caldwell, nice to have you here as well.

I am going to put the clock for 5 and rotate it another 5, so you will have 10, and we will go from there.

STATEMENT OF RAYMOND DECKER, DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT TEAM, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY STEPHEN L. CALDWELL, ASSISTANT DIRECTOR, U.S. GENERAL ACCOUNTING OFFICE

Mr. DECKER. Mr. Chairman and members of the subcommittee, I appreciate the opportunity to be here today to participate in this important hearing on national strategies relating to combating terrorism.

More than 2 years ago, in July 2000, GAO testified before this subcommittee on "Combating Terrorism: The Need for a Strategy." We had just completed our initial review of the Attorney General's Five Year Interagency Counterterrorism and Technology Crime Plan, the closest document to a national strategy at that time, and commented on its weaknesses. We stated at that time, there should be only one national strategy to combat terrorism. We indicated that additional planning guidance providing more detailed information for specific functions should be integrated under this one overarching national strategy in a clear hierarchy.

At that time, Mr. Chairman, you were sponsoring a bill to establish an office that would, among other duties, coordinate a single integrated strategy.

A lot has happened since then. My testimony today is based upon GAO's comprehensive body of work in the area of combating terrorism over the past 6 years at the request of this subcommittee and others. In our past work, we have stressed the importance of a national strategy to combat terrorism which should serve as a foundation for defining what needs to be accomplished, identifying approaches to achieve desired outcomes, and determining how well the goals are being met. It should not only define the roles and missions of the Federal Government and agencies, but also those of State and local government, the private sector and international community. Finally, a national strategy must incorporate sound management principles promoting information sharing and coordination in order to guide effective implementation.

Sir, I'll focus my comments on two areas, the current national strategies and their implementation.

During the last year or so, the administration has developed several new national strategies relating to combating terrorism. This constellation of strategies generally replaces the 1998 Attorney General's Five Year Plan I mentioned earlier. We have identified at least 10 national strategies relating to terrorism; 9 of the 10 are approximately 14 months or younger; 3 are less than a month old. As you can see from the chart on my right, which is also on page 11 of the written statement, we have attempted to portray the complex relationships among these various strategies based on our review of the strategies and discussions with executive branch officials. Please note that the National Drug Control Strategy isn't shown on the chart since its relationship with combating terrorism is mentioned in only one or two areas within that strategy. Also, we are unaware of any national intelligence strategy to combat terrorism tailored to support all of the strategies, although we recognize intelligence and related activities as crucial for their success.

Overall, the strategies do generally form a national framework for combating terrorism. Collectively they provide goals and objectives on broad issues of national security and how combating terrorism and homeland security fit into that larger realm. In addition, they offer more detailed goals and objectives in specific functional areas to include military operations, weapons of mass destruction, money laundering, cyber security, and the protection of physical infrastructure. Although we have not fully evaluated whether the framework these strategies form is cohesive and comprehensive, there are some positive indications. The strategies are organized in a general hierarchy; some share themes, and some explicitly refer to the other strategies. They are more comprehensive in breadth, coverage, and actions needed to combat terrorism than the Attorney General's Five Year Plan. And consistent with our earlier recommendations, the strategies include not just the Federal, but State, local, private, and international partners.

Since the administration has not adopted a single overarching national strategy to combat terrorism and has stated that the National Security and the National Homeland Security Strategy are mutually supporting documents, it's difficult to ascertain the real hierarchy within its framework that may complicate implementation plans. For example, since different Federal agencies have a role in many of these strategies, some confusion in setting priorities and developing coordination mechanisms may exist without a clear understanding of how the strategies are integrated within a tiered framework.

Therefore, we believe that a better defined hierarchy among the various strategies is needed. One approach that better explains the precedence and the interrelationships of the strategies might be with a basic pyramid configuration. Although some blocks might be of different shape and size, a pyramid depiction is somewhat easier to understand for all participants.

For example, might the National Security Strategy of the United States occupy the top-most position on the pyramid and perhaps the National Homeland Security Strategy and National Strategy to Combat Terrorism sharing a tier below.

Mr. Chairman, allow me to briefly comment on implementation. These national strategies, individually or collectively, no matter how well crafted, will not prevent terrorism. However, these documents when implemented through intergovernmental, interagency, and international programs that are seamlessly integrated, effectively coordinated, appropriately resourced, and smartly led will make the difference in the war on terrorism. While these strategies must direct and guide programs, it should be noted that the strategies reflect a host of preexisting initiatives that must be reviewed to ensure proper focus and alignment with newly established goals, objectives, and actions. A critical element for successful implementation is the need for clearly defined roles and responsibilities for all players. If the Federal, State, local, private, and international participants have a thorough understanding of the roles, responsibilities, and capabilities of all involved, then coordination through established mechanisms is greatly facilitated. Finally, leaders at all levels must ensure that the implementation process is effectively and efficiently carried out to achieve goals and objectives within

the time line set. Using essential tools like risk management to guide decisionmaking and performance indicators to gauge progress, leaders will be better able to focus attention and adjust resources to move closer to goals and end states.

Due to the serious consequences of failure, GAO has designated the implementation of homeland security as a high-risk Federal area. This is a product that clearly delineates that challenge. Sir, the leadership challenge is daunting but not impossible.

In closing, we believe the framework formed by these strategies, if effectively implemented with the full involvement and commitment of all partners, will result in significant progress toward our stated goals on the war on terrorism. Congress will play an increasingly important role in addressing the challenges facing this process. In addition to recently passed legislation, reorganizing the Federal Government to combat terrorism, and the appropriation of significant funds to support the war on terrorism, Congress will need to provide keen oversight through hearings like today to ensure all programs are well designed, developed, and executed to accomplish the national goals. Our success on terrorism depends on the leadership and actions of the Federal Government and its domestic and international partners.

Sir, this concludes my prepared statement and I will be pleased to respond to any questions.

Mr. SHAYS. Thank you very much, Mr. Decker.

[The prepared statement of Mr. Decker follows.]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National
Security, Emerging Threats, and International
Relations, Committee on Government
Reform, House of Representatives

For Release on Delivery
Expected at 1:00 p.m. EST
Monday, March 3, 2003

COMBATING TERRORISM

Observations on National Strategies Related to Terrorism

Statement of
Raymond J. Decker, Director
Defense Capabilities and Management



Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to participate in this hearing on national strategies related to combating terrorism. More than 2 years ago, in July 2000, GAO testified before this subcommittee on this very topic and cited concerns over a potential proliferation of overarching national strategies.¹ At that time, we stated that there should be only one national strategy to combat terrorism. We added that additional planning guidance (e.g., at more detailed levels for specific functions) should fall under the one national strategy in a clear hierarchy. My testimony today is based upon GAO's body of work for this and other committees and subcommittees conducted over the past 6 years—much of it related to national strategies and their implementation. At the end of my statement is a list of related GAO products.

Over the last year or so, the administration developed and published several new national strategies related to combating terrorism. This constellation of strategies generally replaces a single strategy issued in December 1998—the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan*—that focused on federal efforts. To date, we have identified 10 other national strategies related to terrorism:

- *National Security Strategy of the United States of America*, September 2002.
- *National Strategy for Homeland Security*, July 2002.
- *National Strategy for Combating Terrorism*, February 2003.
- *National Military Strategy of the United States of America*, September 1997.
- *National Military Strategic Plan for the War on Terrorism*, October 2002.
- *National Strategy to Combat Weapons of Mass Destruction*, December 2002.
- *National Money Laundering Strategy*, July 2002.
- *National Strategy to Secure Cyberspace*, February 2003.
- *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003.
- *National Drug Control Strategy*, February 2002.

In my statement today, after providing some background on the strategies, I will discuss the questions raised in your letter inviting GAO to testify. I have divided the five hearing questions into two major topics. The first major topic addresses whether the new national strategies form a framework that is cohesive and comprehensive. The second major topic addresses whether the strategies will facilitate implementation of programs that are strategy-driven, integrated, and effective. Both topics present difficult questions to answer definitively at this point. The strategies by themselves, no matter how cohesive and comprehensive, will not ensure a strategy-driven, integrated, and effective set of programs to combat terrorism. The ultimate value of these strategies will be in their implementation. Also related to implementation, 9 of the 10 strategies are less than 14 months old, and 3 are less than 1 month old. Notwithstanding these limitations, I will provide GAO's observations to date on these strategies.

¹ U.S. General Accounting Office, *Combating Terrorism: Linking Threats to Strategies and Resources* GAO/T-NSIAD-00-218 (Washington, D.C.: July 26, 2000).

In our past work, we have stressed the importance of a national strategy to combat terrorism.² We stated that such a national strategy should provide a clear statement about what the nation hopes to achieve. A national strategy should not only define the roles of federal agencies, but also those of state and local governments, the private sector, and the international community. A national strategy also should establish goals, objectives, priorities, outcomes, milestones, and performance measures. In essence, a national strategy should incorporate the principles of the Government Performance and Results Act of 1993, which requires federal agencies to set strategic goals, measure performance, and report on the degree to which goals are met.³

SUMMARY

We view the new strategies as a positive step forward. While it will take some time for us to fully evaluate whether they form a cohesive and comprehensive framework, there are some positive indications. The new strategies show cohesion in that they are organized in a hierarchy, share common themes, and cross-reference each other. For example, they provide high-level goals and objectives on the issues of national security in general, and how combating terrorism fits into that larger picture, how to provide for homeland security, and how to combat terrorism overseas. In addition, they provide more detailed goals and objectives for specific functions or areas that include military operations, weapons of mass destruction (WMD), money laundering, cyber security, and the protection of physical infrastructures. In addition, the collective strategies are more comprehensive than the single strategy they generally replace because, consistent with our earlier recommendations, they include not just the federal government, but also state and local governments, the private sector, and the international community.

There will be many challenges to implementing these strategies in a manner that is strategy-driven, integrated, and effective. Given the recency of these strategies, it is premature to evaluate their collective implementation.⁴ Regarding the question of whether these strategies are driving programs, it is important to note that these strategies reflect a host of pre-existing programs: Some of the programs to implement the new strategies have been in place for several years. Nonetheless, the strategies address the implementation of some programs more vigorously than before. Regarding the integration of programs, it is important that federal agencies have clear roles and responsibilities to combat terrorism. Given the number of agencies, it is also important that there be mechanisms to coordinate across agencies. We have identified federal agency roles and responsibilities and coordination mechanisms for both homeland security and combating terrorism overseas and will continue to evaluate their effectiveness. For example, we recently have designated the implementation and

² U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: Sept. 20, 2001).

³ P.L. 103-62 (Aug. 3, 1993).

⁴ However, GAO does have a variety of work recently published or under way to look at more specific strategies and functions related to combating terrorism and homeland security. See the attached list of related GAO products.

transformation of the Department of Homeland Security as a high-risk federal activity. Moreover, implementation must extend beyond the federal level to integrate these efforts with state and local governments, the private sector, and the international community. Regarding the effectiveness of these strategies, performance measures will be important to monitor the successes of programs. One key to assessing overall performance that we previously have identified is that strategies should define an end-state—what the strategies are trying to achieve. Some strategies meet this test, but they generally do not include detailed performance measures. This raises the importance of individual federal agencies having performance measures and reporting their progress. Beyond federal agencies, national measures of success may require a dialogue on appropriate performance measures for state and local governments, the private sector, and the international community. The Congress also has an important role in authorizing, funding, and overseeing the implementation of these strategies to protect the American people from terrorism both at home and abroad.

BACKGROUND ON NATIONAL STRATEGIES RELATED TO TERRORISM

National efforts to combat terrorism derive from a series of presidential directives going back at least as far as 1986. The previous administration issued a federal strategy for combating terrorism—the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan*—in 1998.⁵ The Congress mandated this plan, which was intended to serve as a baseline strategy for coordination of national policy and operational capabilities to combat terrorism both at home and abroad.⁶ The Department of Justice said that plan, in combination with several related presidential directives, represented a comprehensive national strategy. The plan identified several high-level goals aimed at preventing and deterring terrorism, maximizing international cooperation to combat terrorism, improving domestic crisis and consequence planning and management, improving state and local capabilities, safeguarding information infrastructure, and leading research and development efforts to enhance counterterrorism capabilities. The plan set forth efforts by the Department of Justice in partnership with other federal agencies to improve readiness to address the terrorist threat. The Department of Justice issued annual updates to the *Five-Year Plan* in 1999 and 2000, which did not revise the basic plan but tracked agencies' progress in implementing the original plan. More recently, Justice Department officials told us they are no longer providing annual updates because other interagency plans have been released, as discussed below.

In the wake of the terrorist attacks on September 11, 2001, a series of new national strategies were developed and published to help guide U.S. policy. Some of these national strategies are specific to combating terrorism, while others involve terrorism to

⁵ Another earlier and related plan was the *International Crime Control Strategy*, released in May 1998. While not specific to terrorism, this plan had 8 overarching goals and 30 implementing objectives related to international crime. For more information, see U.S. General Accounting Office, *International Crime Control: Sustained Executive-Level Coordination of Federal Response Needed*, GAO-01-629 (Washington, D.C.: Aug. 13, 2001).

⁶ Conference Committee Report (House Report 105-405), Nov. 13, 1997, accompanying the Fiscal Year 1998 Appropriations Act for the Departments of Commerce, Justice, and State; the Judiciary; and related agencies (P.L. 105-119), Nov. 26, 1997.

lesser degrees. Table 1 describes various national strategies related to combating terrorism.

Table 1: National Strategies Related to Combating Terrorism

Strategy	Description of strategy
<p><i>National Security Strategy of the United States of America</i></p> <ul style="list-style-type: none"> • Issued by the President, September 2002 	<p>This document provides a broad framework for strengthening U.S. security in the future. It identifies the national security goals of the United States, describes the foreign policy and military capabilities necessary to achieve those goals, evaluates the current status of these capabilities, and explains how national power will be structured to utilize these capabilities. It devotes a chapter to combating terrorism that focuses on the disruption and destruction of terrorist organizations, the winning of the “war of ideas,” the strengthening of homeland security, and the fostering cooperation with allies and international organizations to combat terrorism.</p>
<p><i>National Strategy for Homeland Security</i></p> <ul style="list-style-type: none"> • Issued by the President, July 2002 	<p>This document addresses the threat of terrorism within the United States by organizing the domestic efforts of federal, state, local, and private organizations. Although mostly domestic in focus, this strategy mentions various initiatives related to combating terrorism overseas, including: negotiating new international standards for travel documents, improving security for international shipping containers, enhancing cooperation with foreign law enforcement agencies, expanding specialized training and assistance to allies, and increasing the security of transnational infrastructure. The strategy stresses the importance of expanding international cooperation in research and development and enhancing the coordination of incident response. Finally, the strategy recommends reviewing current international treaties and law to determine where improvements could be made.</p>

<p><i>National Strategy for Combating Terrorism</i></p> <ul style="list-style-type: none"> • Issued by the President, February 2003 	<p>This document elaborates on the terrorism aspects of the <i>National Security Strategy of the United States of America</i> by expounding on the need to destroy terrorist organizations, win the “war of ideas,” and strengthen security at home and abroad. Unlike the <i>National Strategy for Homeland Security</i> that focuses on preventing terrorist attacks within the United States, the <i>National Strategy for Combating Terrorism</i> focuses on identifying and defusing threats before they reach the borders of the United States. In that sense, although it has defensive elements, this strategy is an offensive strategy to complement the defensive <i>National Strategy for Homeland Security</i>.</p>
<p><i>National Military Strategy of the United States of America</i></p> <ul style="list-style-type: none"> • Issued by the Chairman of the Joint Chiefs of Staff, September 1997 	<p>This document sets the strategic direction for all aspects of the Armed Forces. This includes force structure, acquisition, and doctrine as well as the strategic environment. The 1997 strategy notes the rising danger of asymmetric threats, such as terrorism. The strategy stresses the need for the military to adapt its doctrine, training, and equipment to ensure a rapid and effective joint and interagency response to these threats.</p>
<p><i>National Military Strategic Plan for the War on Terrorism</i></p> <ul style="list-style-type: none"> • Issued by the Chairman of the Joint Chiefs of Staff, October 2002 	<p>This document provides a framework to guide the conduct of the “war on terrorism” by U.S. Armed Forces. It provides specific guidance from which regional commanders, the military services, and other agencies can formulate their own individual action plans. Individual regional commands drafted their own campaign plans in response to this plan. For example, one regional command plans to conduct maritime interception operations to disrupt terrorists’ use of commercial shipping to transport people and material.</p>
<p><i>National Strategy to Combat Weapons of Mass Destruction</i></p> <ul style="list-style-type: none"> • Issued by the President, December 2002 	<p>This document presents a national strategy to combat weapons of mass destruction through three major efforts: (1) nonproliferation, (2) counterproliferation, and (3) consequence management in WMD incidents. The plan addresses the production and proliferation of weapons of mass destruction among states, as well as the potential threat of terrorists using WMD agents.</p>

<p><i>National Money Laundering Strategy</i></p> <ul style="list-style-type: none"> • Issued by the Secretary of the Treasury and the Attorney General, July 2002 	<p>This document is intended to support planning for the efforts of law enforcement agencies, regulatory officials, the private sector, and overseas entities to combat the laundering of money generated from criminal activities. Although the 2002 strategy still addresses general criminal financial activity, that plan is the first to outline a major governmentwide strategy to combat terrorist financing. The strategy discusses the need to adapt traditional methods of combating money laundering to unconventional tools used by terrorist organizations to finance their operations.</p>
<p><i>National Strategy to Secure Cyberspace</i></p> <ul style="list-style-type: none"> • Issued by the President, February 2003 	<p>This document is intended to provide an initial framework for both organizing and prioritizing efforts to protect our nation's critical cyber infrastructures. Also, it is to provide direction to federal departments and agencies that have roles in cyberspace security and to identify steps that state and local governments, private companies and organizations, and individual Americans can take to improve the nation's collective cybersecurity. The strategy is organized according to five national priorities, with major actions and initiatives identified for each. These priorities are: (1) a National Cyberspace Security Response System, (2) a National Cyberspace Security Threat and Vulnerability Reduction Program, (3) a National Cyberspace Security Awareness and Training Program, (4) Securing Governments' Cyberspace, and (5) National Security and International Cyberspace Security Cooperation. In describing the threats and vulnerabilities for our nation's cyberspace, the strategy highlights the potential for damage to U.S. information systems from attacks by overseas terrorist organizations.</p>

<p><i>National Strategy for the Physical Protection of Critical Infrastructures and Key Assets</i></p> <ul style="list-style-type: none"> • Issued by the President, February 2003 	<p>This document provides a statement of national policy to remain committed to protecting critical infrastructures and key assets from terrorist attacks, and it is based on eight guiding principles, including establishing responsibility and accountability, encouraging and facilitating partnering among all levels of government and between government and industry, and encouraging market solutions wherever possible and government intervention when needed. The strategy also establishes three strategic objectives. The first is to identify and assure the protection of the most critical assets, systems, and functions, in terms of national-level public health and safety, governance, and economic and national security and public confidence. The second is to assure protection of infrastructures and assets facing specific, imminent threats. The third is to pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time.</p>
<p><i>National Drug Control Strategy</i></p> <ul style="list-style-type: none"> • Issued by the President, February 2002 	<p>This document sets specific national goals for reducing drug use in America. The report underscores the need for international law enforcement cooperation to combat this problem. Although the plan does not directly deal with combating terrorism, it highlights drug revenue as a source of funding for 12 of the 28 international terrorist groups identified by the Department of State.</p>

Source: Published national strategies.

Note: GAO analysis of published national strategies.

Some Strategies Define Terrorism and Include an Assessment of the Threat

The *National Security Strategy of the United States of America*, the *National Strategy for Combating Terrorism*, and the *National Strategy for Homeland Security* all define terrorism. For example, the *National Strategy for Homeland Security* characterizes terrorism as “any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments.” This description, according to that strategy, captures the core concepts shared by the various definitions of terrorism contained in the U.S. Code, each crafted to achieve a legal standard of specificity and clarity. This description covers kidnappings; hijackings; shootings; conventional bombings; attacks involving chemical, biological, radiological, or nuclear weapons; cyber attacks; and any number of other forms of malicious violence. Terrorists can be U.S. citizens or foreigners, acting in concert with others, on their own, or on behalf of a hostile state.

Commonly accepted definitions of such terms as terrorism and homeland security help provide assurance that organizational, management, and budgetary decisions are made consistently across the organizations involved in a crosscutting effort. For example, they help guide agencies in organizing and allocating resources and can help promote more effective agency and intergovernmental operations by facilitating communication. A common definition also can help to enforce budget discipline and support more accurate monitoring of expenditures. Without commonly accepted definitions, the potential exists for an uncoordinated approach to combating terrorism caused by duplication of efforts or gaps in coverage, misallocation of resources, and inadequate monitoring of expenditures. We previously recommended that the President direct the Office of Homeland Security to (1) develop a comprehensive, governmentwide definition of homeland security and (2) include the definition in the [then] forthcoming national strategy.⁷ Both recommendations were implemented with the publication of the *National Strategy for Homeland Security*.

As we have testified before this subcommittee, an important step in developing sound strategies to combat terrorism is to develop a thorough assessment of the terrorist threat. Intelligence and law enforcement agencies continuously assess the foreign and domestic terrorist threats to the United States. To be considered a threat, a terrorist group must not only exist, but also have the intention and capability to launch attacks.⁸ In prior reports, we have recommended that the federal government conduct multidisciplinary and analytically sound threat assessments. Threat assessments are part of a risk management approach that can be used to establish requirements and prioritize program investments.⁹ In 1999 we recommended that the Federal Bureau of Investigation (FBI) conduct a national-level authoritative threat assessment.¹⁰ According to FBI officials, they have recently completed their threat assessment related to our recommendation. We are in the process of reviewing the assessment to determine the extent it is consistent with our recommendation. We hope that such an assessment will be kept up to date and used to further develop and implement the new national strategies related to combating terrorism.

Some of the new strategies we reviewed include some assessment of the threat. While some of the new strategies lay out the nature of the threats and the vulnerabilities in detail, others briefly describe the threat in general terms. For example, the *National Strategy for Combating Terrorism* discusses the nature of the terrorist threat today, including the structure of terrorism, the changing nature of terrorism, the interconnected

⁷ U.S. General Accounting Office, *Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains*, GAO-02-610 (Washington, D.C.: June 7, 2002).

⁸ Other factors to consider in analyzing threats include a terrorist group's history, its targeting, and the security environment in which it operates.

⁹ For more information on a risk management approach, see U.S. General Accounting Office, *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74 (Washington, D.C.: Apr. 9, 1998) and U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001).

¹⁰ U.S. General Accounting Office, *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks*, GAO/NSIAD-99-163 (Washington, D.C.: Sept. 7, 1999).

terrorist organizations, the availability of weapons of mass destruction, and the new global environment. Some strategies describe both the threat of and vulnerability to terrorist attacks. For example, the *National Strategy to Secure Cyberspace* discusses cyberspace threats and vulnerabilities facing the United States. It lays out the threats and vulnerabilities as a five-level problem—home user/small business, large enterprises, critical sectors and/or infrastructures, national issues and vulnerabilities, and global. Also, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and the *National Strategy for Homeland Security* discuss both the threat and vulnerability of a terrorist attack. Other strategies we reviewed only briefly described the threat or simply defined the threat in general terms. For example, the *National Strategy to Combat Weapons of Mass Destruction* defined the threat, while the *National Money Laundering Strategy* provided limited discussion about the nature and extent of the threat.

NEW STRATEGIES FORM FRAMEWORK

Now I will discuss the key topics that the subcommittee wants to address in this hearing, starting with the question of whether the new national strategies form a cohesive and comprehensive framework. While it will take some time for us to fully answer this question, we view the new strategies, and the framework they provide, as a positive step. The new strategies show cohesion in that they are organized in a hierarchy, share common themes, and cross-reference each other. In addition, the collective strategies are more comprehensive than the single strategy they generally replace because they include more detailed functions and more players.

New Strategies Show Cohesion Through Hierarchy, Common Themes, and Linkages

In our analysis, we found specific indicators that the strategies form a cohesive framework. For the purpose of this testimony, we are defining cohesiveness as the extent that the strategies have some hierarchy, share common themes, and link to each other.

Regarding a hierarchy among strategies, I would like to again reference our July 2000 testimony. At that time, we stated that there should be one national strategy to combat terrorism with additional planning guidance (e.g., for specific functions) under the one strategy in a clear hierarchy.¹¹ While the administration has not taken that exact path, its approach is similar. The *National Security Strategy of the United States of America* provides the overarching strategy related to national security as a whole, including terrorism. The *National Strategy for Homeland Security* and the *National Strategy for Combating Terrorism* provide, respectively, the more specific strategies related to combating terrorism at home and overseas. This differs from what we had envisioned in that there are two top-level strategies dedicated to terrorism instead of one. However,

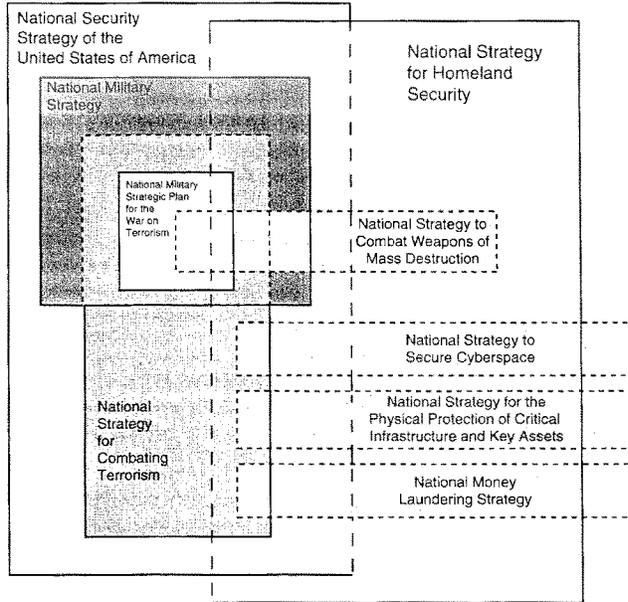
¹¹ In that testimony, we also cited the potential danger from a proliferation of overarching national strategies to combat terrorism. At that time, the National Security Council and the FBI were planning to develop national strategies that would potentially compete with the Attorney General's *Five-Year Counterterrorism and Technology Crime Plan*. The recent constellation of new strategies generally is coordinated out of the Executive Office of the President or addresses different specific functions or subsets of combating terrorism.

this approach is consistent with our earlier views because the two strategies cover separate topics—the first covers defensive domestic issues and the second covers offensive overseas issues.¹² The other strategies provide further levels of detail on the specific functions related to military operations, money laundering, weapons of mass destruction, cyber security, and protection of physical infrastructure.

Our interpretation of the hierarchy among strategies is somewhat different from how the administration has presented it. According to the administration, the *National Security Strategy of the United States of America* and the *National Strategy for Homeland Security* are top-level strategies that together address U.S. security both overseas and domestically. According to the administration, these two strategies establish a framework that takes precedence over *all* other national strategies, plans, and programs. However, we do not view the hierarchy as that absolute because some strategies contain independent elements that do not overlap with the other strategies. For an example of the latter, both the *National Strategy to Secure Cyberspace* and the *National Money Laundering Strategy* include some domestic criminal elements not associated with national security or terrorism. Further, the *National Drug Control Strategy* has relatively little overlap with these other strategies. Figure 1 is an attempt to display graphically how some of these national strategies fit into a hierarchy and overlap.

¹² We recognize that this characterization of the strategies simplifies a complex relationship between the two. Both strategies contain both defensive and offensive elements. For example, while we characterize the *National Strategy for Homeland Security* as mainly defensive, it includes offensive initiatives to target and attack terrorist financing, and to track foreign terrorists and bring them to justice. Similarly, while we characterize the *National Strategy for Combating Terrorism* as mainly offensive, it includes defensive objectives to implement the *National Strategy for Homeland Security* and to protect U.S. citizens abroad.

Figure 1: Relationships between and among National Strategies Related to Combating Terrorism



Source: Published national strategies.

Note: This graphic is intended to show relationships and overlaps among these national strategies. The sizes and shapes of the boxes are not meant to imply the relative importance of all the strategies.

Within the hierarchy of strategies, more detailed functional strategies might be useful, as illustrated by the *National Strategy to Combat Weapons of Mass Destruction*. In our August 2002, report on the Department of Energy's National Nuclear Security Agency's research and development (R&D) program, we recommended that the Office of Homeland Security clarify that agency's Nonproliferation and Verification R&D Program's role in relation to other agencies conducting counterterrorism R&D and to achieve an appropriate balance between short-term and long-term research.¹⁵ We also reported that there is a conflict among Department of Energy laboratories between short- versus long-term research and that this conflict has created a gap in which the most important immediate needs of users, or highest risks, are in some cases going

¹⁵ U.S. General Accounting Office *Nonproliferation R&D: NNSA's Program Develops Successful Technologies, but Project Management Can Be Strengthened*, GAO-02-904 (Washington, D.C.: Aug. 23, 2002).

unaddressed in favor of an advanced technology that only can be delivered over the long term. The *National Strategy to Combat Weapons of Mass Destruction* addresses our concerns, in part, by noting that the new Counterproliferation Technology Coordination Committee will act to improve interagency coordination of U.S. government counterproliferation research and development efforts. The committee is expected to assist in identifying gaps and overlaps in existing programs and in examining options for future investment strategies.

The various strategies also show cohesion by sharing common themes. For example, nearly all of the strategies contain either goals or objectives relating to strengthening international relationships and cooperation and strengthening intelligence gathering and analysis capabilities, while just over half of the strategies contain either goals or objectives relevant to the strengthening of capabilities to deter, prevent, and respond to weapons of mass destruction. Moreover, among the four strategies most relevant to homeland security—the *National Strategy for Homeland Security*, the *National Strategy for Physical Protection of Critical Infrastructures and Key Assets*, the *National Strategy to Secure Cyberspace*, and the *National Money Laundering Strategy*—all contain a number of additional, similar themes. With the exception of the *National Money Laundering Strategy*, which does not address critical infrastructure and key asset protection, all of these homeland security-related strategies contain either goals or objectives aimed at strengthening intergovernmental and private sector relationships, critical infrastructure and key asset protection, and information-sharing capabilities. Similarly, among the strategies more relevant to combating terrorism overseas—such as the *National Security Strategy of the United States of America*, the *National Strategy for Combating Terrorism*, the *National Strategy to Combat Weapons of Mass Destruction*, and the *National Military Strategy of the United States of America*—all contain either goals or objectives relating to strengthening international relationships; strengthening intelligence gathering and analysis capabilities; and improving capabilities to deter, prevent, and respond to weapons of mass destruction. As mentioned earlier, the *National Drug Control Strategy* has relatively little overlap with the other strategies. It does not share many of these themes—with the exception of strengthening border control capabilities and, to some extent, the strengthening of international relationships and cooperation.

In addition, the strategies show evidence of cohesion through linkages among them. These linkages occur through specific citations and cross-references from one document to another. At least half of the strategies cite either the *National Security Strategy of the United States of America* or the *National Strategy for Homeland Security*. The most extensively linked strategies include the *National Security Strategy of the United States of America*, the *National Strategy for Homeland Security*, the *National Strategy for Combating Terrorism*, and the *National Strategy to Combat Weapons of Mass Destruction*. Strategies that cover topics beyond terrorism, such as criminal law enforcement, are less extensively linked to these documents. For example, the *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* solely cite each other and the *National Strategy for Homeland Security*. The *National Drug Control Strategy* and the *National Money Laundering Strategy* contain no explicit linkages to any of the other strategies, but are

referenced in the *National Strategy for Homeland Security*. There are some areas where linkages could be improved. For example, the *National Strategy for Homeland Security* is the only strategy to explicitly cite virtually all of the strategies and explain their relationships to it and to one another. Some strategies contain broad themes that are covered in more detail by other strategies, but do not cite these documents. For instance, although the *National Strategy for Combating Terrorism* mentions the topic of terrorist financing, it does not mention the *National Money Laundering Strategy*. Nevertheless, it mentions the *National Drug Control Strategy*, a document with considerably less thematic overlap in terms of terrorism. The *National Security Strategy of the United States of America* covers many broad strategic themes, but refers to no other national strategies, although many of the strategies refer back to it.

New Strategies Include Key Functions and Organizations

Potential indicators of comprehensiveness are whether the strategies include all relevant functions and organizations. As stated earlier, they collectively provide not only the broader context of combating terrorism, but also the more detailed strategies for the functions of military operations, money laundering, weapons of mass destruction, cyber security, and protection of physical infrastructure. While parts of the strategies overlap, GAO has not yet done a complete analysis to determine whether gaps exist in the collective coverage of these strategies. However, some of our work for this subcommittee indicates that intelligence is a critical function that cuts across all the other strategies, but does not have a strategy itself related to terrorism, at least according to CIA officials with whom we spoke.

Regarding the inclusion of all relevant organizations, the collective strategies are more comprehensive than the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan* that they generally replaced. In our September 2001 report on combating domestic terrorism, we had characterized this plan as a "federal" plan and not a "national" plan because it did not include state and local governments, where appropriate.¹⁴ In addition, our more recent work on homeland security stressed the need for partnerships with state and local governments and the private sector.¹⁵ Consistent with GAO's earlier findings and recommendations, some of the new strategies include not just the federal government, but also these other players as well as the international community.

POTENTIAL CHALLENGES IN IMPLEMENTING THE STRATEGIES

The strategies by themselves, no matter how cohesive and comprehensive, will not ensure a strategy-driven, integrated, and effective set of programs to combat terrorism. The ability to ensure these things will be determined through time as the strategies are implemented. Given that these strategies are relatively new, GAO has not yet evaluated

¹⁴ See GAO-01-822.

¹⁵ U.S. General Accounting Office, *Homeland Security: Management Challenges Facing Federal Leadership*, GAO-03-260 (Washington, D.C.: Dec. 20, 2002).

their implementation, either individually or collectively. However, we have done work that demonstrates the federal government, and the nation as a whole, will face many implementation challenges. For example, we have designated the implementation and transformation of the Department of Homeland Security as a high-risk federal activity. The Congress also will play a key role in implementing these strategies.

New Strategies Reflect Long-Standing Programs

Regarding the question of whether these strategies are driving programs, it is important to note that these new strategies reflect a host of pre-existing programs. For example, certain themes and related programs contained in the new strategies—preventing and deterring terrorism, maximizing international cooperation to combat terrorism, improving domestic crisis and consequence planning and management, improving state and local capabilities, safeguarding information infrastructure, and leading research and development efforts to enhance counterterrorism capabilities—were included in the Attorney General's *Five-Year Interagency Counterterrorism and Technology Crime Plan*. Some of the related policies and programs have been in place for several years. For example, the State Department's Antiterrorism Assistance Program, which provides assistance to other countries to improve their capabilities, has existed since 1983. In another example, federal assistance programs for state and local first responders to help them prepare to respond to weapons of mass destruction—the Nunn-Lugar-Domenici training—was established in 1996.

Implementation Requires Integration Among Many Sectors

Integrating federal agencies is a major challenge in implementing the new strategies. It is important, for example, that federal agencies have clearly defined roles and responsibilities. The new strategies define the roles and responsibilities of agencies for functional areas to varying degrees. Some of the strategies described lead agency roles responsibilities in detail. For example, the *National Strategy for Homeland Security* described lead agency responsibilities for various functional areas, such as intelligence and warning, border and transportation security, and protecting critical infrastructure and key assets. Other strategies, including the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and the *National Money Laundering Strategy*, also identified key agencies' roles and responsibilities in leading various functional areas. Other strategies we reviewed either were silent in terms of identifying agencies to lead functional areas or only generally described agency roles and responsibilities. For example, the *National Strategy to Combat Weapons of Mass Destruction* focused more on areas of national priorities and initiatives and did not identify agency roles and responsibilities. In addition, the *National Strategy for Combating Terrorism* only briefly identified lead functional areas for agencies. We recognize that documents other than these strategies, such as presidential directives, also assign agency roles.

A key component in integrating federal agencies is interagency coordination. While the strategies generally do not address such coordination mechanisms, we identified them for both homeland security and combating terrorism overseas. Homeland security is

coordinated through the Office of Homeland Security and the Homeland Security Council, which have 11 interagency working groups (called policy coordination committees) to manage crosscutting issues in such areas as detection, surveillance, and intelligence; law enforcement and investigation; and WMD consequence management. The Department of Homeland Security is responsible for coordination with other federal agencies, state and local governments, and the private sector. In addition, the new department will serve a coordination role by consolidating several agencies that currently are under separate departments. In combating terrorism overseas, the National Security Council plays a major coordinating role by sponsoring a policy coordination committee called the Counterterrorism Security Group, which has several subordinate interagency working groups on such topics as interagency exercises and assistance to other countries. Coordination overseas occurs in other ways as well, through interagency groups at U.S. embassies and regional military commands.

The challenge of integration goes beyond the federal level to include state and local governments, the private sector, and the international community. As mentioned earlier, the strategies do address these other entities, but in varying degrees of detail. For example, the *National Strategy for Homeland Security* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* provide extended discussions of the importance of partnerships among various federal agencies, state and local governments, the private sector, and to a lesser degree, the international community. In contrast, the *National Security Strategy of the United States of America* discusses the role of the international community in more general terms.

New Strategies Generally Do Not Include Performance Measures

Performance measures are important for monitoring the successes of strategies and their related programs. One key to assessing overall performance that we have previously called for in strategies is that they define an end-state—what a strategy is trying to achieve. Some of these strategies do this, although the clarity of their end-states varies considerably. For instance, the *National Strategy for Combating Terrorism* details a very specific desired end-state where the scope and capabilities of global terrorist organizations are reduced until they become localized, unorganized, unsponsored, and rare enough that they can be dealt with exclusively by criminal law enforcement. Other end-states focus on federal capabilities, rather than the terrorist target. For example, the *National Strategy for Homeland Security* stresses the need for a fully integrated national emergency response system that is adaptable enough to deal with any terrorist attack, no matter how unlikely or catastrophic. Finally, some end-states are more strategic in nature, the prime example belonging to the *National Security Strategy of the United States of America*, which seeks to create a “balance of power that favors human freedom: conditions in which all nations and all societies can choose for themselves the rewards and challenges of political and economic liberty.”

Although some strategies identify an end-state, most strategies lack detailed performance goals and measures to monitor and evaluate the success of combating terrorism programs. In our past work concerning a national strategy for homeland security, we said the national strategy should establish explicit national objectives,

outcome-related goals, and performance measures to guide the nation's homeland security efforts. This approach would provide a clearer statement on what the nation hopes to achieve through its programs to combat terrorism. The strategies generally describe overarching objectives and priorities, but not measurable outcomes. More explicit actions or initiatives in some of the plans begin to provide a greater sense of what is expected, but these often are in the form of activities or processes, which are not results-oriented outcomes. For example, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* discusses coordinating and consolidating federal and state protection plans, but does not give a clear description of the result of such coordination and consolidation. The *National Money Laundering Strategy* devotes a section to measuring effectiveness and calls for developing measures and institutionalizing systems for such measures.

The general lack of specific performance goals and measures in the strategies makes it more important that individual federal agencies have explicit performance goals and related measures. The primary vehicle for setting federal strategic and annual performance goals is the Government Performance and Results Act of 1993, commonly referred to as GPRA or the Results Act.¹⁶ The Results Act provides agencies with a systematic approach for managing programs. The Results Act's principles include clarifying missions, developing a strategy, identifying goals and objectives, and establishing performance measures. We believe that federal agencies with national strategy responsibilities should address them through the Results Act process.

The Department of State is an example of an individual agency that has performance measures related to combating terrorism. The department's *Performance Plan for Fiscal Year 2003* specifically identifies countering terrorism as one of the department's strategic goals. The goal is to reduce international terrorist attacks, especially against the United States and its citizens. To measure its progress toward achieving this goal, the department identified the following performance indicators and targets for fiscal year 2003:

- Some 25 bilateral and multilateral counterterrorism consultations will be completed.
- Some 96 countries will implement United Nations Security Council Resolution 1373, which requires all member states to suppress and prevent terrorism.
- Some 210 Antiterrorism Assistance training courses will be provided to 60 countries, with all programs reviewed within 18 months after the training. This training is expected to increase the ability of key countries to fight terrorism.
- The Foreign Emergency Support Team will deploy to participate in two of the Combatant Commanders' International Counterterrorism Exercises.
- All of the reviews of foreign terrorist organizations will be completed within 1 year.

Beyond federal agencies, national goals and measures of success may warrant a dialogue about performance goals and measures for nonfederal partners—state and local governments, the private sector, and the international community. In the absence of

¹⁶ P.L. 103-62 (Aug. 3, 1993).

definitive nonfederal goal and measurement approaches, we believe there is a strong potential the national strategies will revert to primarily a federal responsibility. While this is a difficult area given federalism principles, international sovereignty, and private sector independence, national strategies to combat terrorism require national (and international) performance expectations if they are to be successfully implemented.

Many Other Management Issues Will Make Implementation a Challenge

In addition to the implementation issues in the subcommittee's letter—whether implementation will be strategy-driven, integrated, and effective—we have identified several other management challenges. Our previous work regarding homeland security and the establishment of the Department of Homeland Security raised several issues that are applicable to implementing the new strategies.¹⁷ We designated the implementation and transformation of the department as a high risk for three reasons. First, the size and complexity of the effort make the challenge especially daunting, requiring sustained attention and time to achieve the department's mission in an effective and efficient manner. Second, components being merged into the department already face a wide variety of existing challenges that must be addressed. Finally, the department's failure to effectively carry out its mission exposes the nation to potentially very serious consequences.

Successful implementation will require adherence to certain management practices and key success factors. These factors include strategic planning, risk management, information technology management, human capital strategy and management, and a variety of other critical management processes and tools that will improve opportunities for achieving significant combating-terrorism objectives. For example, strong financial management will be necessary to assure accountability over significant direct and indirect federal expenditures. Improvements in leveraging information technology also will be necessary to not only enhance the effective utilization of management systems, but also to increase information sharing among and between all parties. Additionally, implementing the strategic framework for combating terrorism will require addressing key, specific federal management capabilities. Some of the federal departments and agencies assigned to carry out the strategy face management challenges in administering their programs, managing their human capital, and implementing and securing information technology systems. Federal agencies will need to address these challenges as well as develop or enhance specific homeland security management capabilities, such as identifying threats, risks, vulnerabilities, and responses and effectively working in interagency, intergovernmental, and private sector relationships.

Similarly, we must recognize that a number of agencies will face challenges in meeting dual or unrelated missions while maintaining and strengthening their combating terrorism operations. Additional actions to clarify missions and activities will be necessary, and some agencies will need to determine how best to support both

¹⁷ U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: Jan. 2003); GAO-03-260; and U.S. General Accounting Office, *Highlights of a GAO Forum: Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies*, GAO-03-293SP (Washington, D.C.: Nov. 14, 2002).

combating terrorism and non-combating terrorism missions. For example, in a recent report we raised issues regarding the need for the Federal Emergency Management Agency and U.S. Coast Guard—both now part of the Department of Homeland Security—to balance multiple missions.¹⁸ Creating an effective structure that is sensitive to balancing the needs of homeland security and non-homeland security functions will be critical to the successful implementation of the strategies.

Finally, many agencies tasked with carrying out the initiatives and objectives of the various strategies have long-standing human capital problems that will need to be addressed. One of these challenges has been the ability to hire and retain a talented and motivated staff. For example, we reported that the Immigration and Naturalization Service was unable to reach its program goals in large part because of such staffing problems as hiring shortfalls and agent attrition.¹⁹ Moreover, to accomplish national and homeland security missions some agencies have recognized the need for new skills in the workforce. It is anticipated that agencies will need employees skilled in information technology, law enforcement, foreign languages, and other proficiencies. For example, we have reported that the FBI has an action plan to hire translators, interpreters, and special agents with language skills—areas where the federal government currently has a shortage.²⁰

The Next Steps In Implementing Programs to Combat Terrorism

To implement the new constellation of national strategies, we see some additional next steps that should be taken. These are based upon our body of work on federal programs to combat terrorism. Among other unfinished business, the Executive Branch will have to (1) establish and refine performance measures, (2) establish milestones for completing tasks, (3) link resources to threats and strategies, and (4) use a risk management approach.

The Congress Will Play an Important Role in Implementing the Strategies

The Congress will play an important role as well in addressing the challenges faced in implementing these strategies. The Congress recently passed legislation reorganizing the federal government to combat terrorism by creating the Department of Homeland Security. The Congress will be appropriating funds—billions of dollars—to that department and other federal agencies that combat terrorism. And finally, the Congress will need to provide oversight, in hearings like this one today, to ensure that the programs are appropriately designed and implemented. GAO will continue to assist this subcommittee, and the Congress as a whole, in helping the federal government develop and implement programs to protect the United States from terrorism both at home and abroad.

¹⁸ GAO-03-102.

¹⁹ U.S. General Accounting Office, *Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy*, GAO-02-861T (Washington, D.C.: June 19, 2002).

²⁰ U.S. General Accounting Office, *Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls*, GAO-02-375 (Washington, D.C.: Jan. 31, 2002).

This concludes my prepared statement. I will be pleased to respond to any questions that you or other members of the subcommittee may have.

GAO CONTACTS AND STAFF ACKNOWLEDGMENTS

For future contacts about this statement, please contact Raymond J. Decker at (202) 512-6020. Individuals making key contributions to this statement include Stephen L. Caldwell, Mark A. Pross, Sharon L. Caudle, James C. Lawson, David W. Hancock, Michael S. Arbogast, Susan K. Woodward, Edward T. Staples, and David S. Epstein.

Related GAO Products

Major Management Challenges and Program Risks: Department of Homeland Security. GAO-03-102. Washington, D.C.: January 2003.

Homeland Security: Management Challenges Facing Federal Leadership. GAO-03-260. Washington, D.C.: December 20, 2002.

Combating Terrorism: Funding Data Reported to Congress Should Be Improved. GAO-03-170. Washington, D.C.: November 26, 2002.

Highlights of a GAO Forum: Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies. GAO-03-293SP. Washington, D.C.: November 14, 2002.

Homeland Security: Effective Intergovernmental Coordination Is Key to Success. GAO-02-1013T. Washington, D.C.: August 23, 2002.

Nonproliferation R&D: NNSA's Program Develops Successful Technologies, but Project Management Can Be Strengthened. GAO-02-904. Washington, D.C.: August 23, 2002.

Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy. GAO-02-861T. Washington, D.C.: June 19, 2002.

Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains. GAO-02-610. Washington, D.C.: June 7, 2002.

Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls. GAO-02-375. Washington, D.C.: Jan. 31, 2002.

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts. GAO-02-208T. Washington, D.C.: October 31, 2001.

Combating Terrorism: Selected Challenges and Related Recommendations. GAO-01-822. Washington, D.C.: September 20, 2001.

International Crime Control: Sustained Executive-Level Coordination of Federal Response Needed. GAO-01-629. Washington, D.C.: August 13, 2001.

Combating Terrorism: Observations on Options to Improve the Federal Response. GAO-01-660T. Washington, D.C.: April 24, 2001.

Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy. GAO-01-556T. Washington, D.C.: March 27, 2001.

Combating Terrorism: Federal Response Teams Provide Varied Capabilities: Opportunities Remain to Improve Coordination. GAO-01-14. Washington, D.C.: November 30, 2000.

Combating Terrorism: Linking Threats to Strategies and Resources. GAO/T-NSIAD-00-218. Washington, D.C.: July 26, 2000.

Combating Terrorism: Comments on Bill H.R. 4210 to Manage Selected Counterterrorist Programs. GAO/T-NSIAD-00-172. Washington, D.C.: May 4, 2000.

Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism. GAO/NSIAD-00-85. Washington, D.C.: April 7, 2000.

Combating Terrorism: Issues in Managing Counterterrorist Programs. GAO/T-NSIAD-00-145. Washington, D.C.: April 6, 2000.

Combating Terrorism: Observations on the Threat of Chemical and Biological Terrorism. GAO/T-NSIAD-00-50. Washington, D.C.: October 20, 1999.

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks. GAO/NSIAD-99-163. Washington, D.C.: September 7, 1999.

Combating Terrorism: Issues to Be Resolved to Improve Counterterrorism Operations. GAO/NSIAD-99-135. Washington, D.C.: May 13, 1999.

Combating Terrorism: Observations on Federal Spending to Combat Terrorism. GAO/T-NSIAD/GGD-99-107. Washington, D.C.: March 11, 1999.

Combating Terrorism: Observations on Crosscutting Issues. GAO/T-NSIAD-98-164. Washington, D.C.: April 23, 1998.

Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments. GAO/NSIAD-98-74. Washington, D.C.: April 9, 1998.

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination. GAO/NSIAD-98-39. Washington, D.C.: December 1, 1997.

Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy. GAO/NSIAD-97-254. Washington, D.C.: September 26, 1997.

(350329)

Mr. SHAYS. Just for the benefit of new Members here—and first let me welcome Congressman Chris Bell from Texas, a new member to the committee. We are delighted that you are a member of this committee. I think you will find the work of this committee quite meaningful and helpful to your district and our country. At this time, Mr. Bell, I would be happy to recognize if you would like to make an opening statement.

Mr. BELL. Thank you very much, Mr. Chairman. I very much appreciate the opportunity to serve with you on this committee. And I thank you for calling this hearing on what has obviously become one of our Nation's top priorities, finding a way to combat terrorism and securing the homeland. And I would like to thank Mr. Decker and the others who will be testifying here today and offer themselves to answer our questions.

I have some questions about the plan, but I will hold off on those until it becomes my time, but I thank you for the opportunity. And thanks for your welcoming remarks as well.

Mr. SHAYS. What we usually do in this committee is 10 minutes if we have two or three members. But what we'll do is first do a 5-minute round and then we'll come back and if someone needs to go over the 5 minutes or wants to do a second round, we'll do another round. And I have a rusty staff that didn't turn on the clock for you, Mr. Decker, but don't blame the clock. So here we go. Mr. Decker, I want to ask you to describe in very short terms why a strategy is important.

Mr. DECKER. Sir, very simply, this strategy is the foundation piece in which you can go and implement particular plans and actions and make sure that they achieve some type of end state. I have used strategies, and I think most professionals will look at them as road maps or concept papers, that give you an idea of what has to be accomplished, what is in the Nation's best interest, and, in a general way, how to go about doing that.

So if you have a good strategy, you're off to a good start, because from that you can derive many other vehicles and tools that will help you do what you need to do.

Mr. SHAYS. Thank you. You have come before this committee before September 11th, as have all three commissions dealing with terrorism. And all three, the Gilmore, the Bremmer, the Hart-Rudman Commission, made these three points. They said there's a new threat out there. They said you need to develop a new strategy. And then they said that you need to reorganize your government accordingly. And I think the only area they disagreed was on the reorganization of government.

When we encountered an ally in the Soviet Union—former ally of the Soviet Union becoming our enemy, they wanted to destroy us politically, socially, economically, as well as militarily, we brought people in and President Truman and then President Eisenhower—but with President Eisenhower, he brought them into the White House; and it was basically called the Solarium Project, and they developed the fact that we needed a new strategy which was basically one of containment and reactive and mutually assured destruction.

You accept the fact that strategy is no longer viable with today's threat?

Mr. DECKER. Sir, it's difficult to answer. I don't think we've done—

Mr. SHAYS. I am not asking you what it should be. It's not difficult to answer. Is that old strategy going to be effective against this war on terrorism? This isn't a trick question.

Mr. DECKER. No, sir. I understand—

Mr. SHAYS. Let me put it this way. Do you agree with all three Commissions that said we needed a new strategy?

Mr. DECKER. Yes, sir.

Mr. SHAYS. So the answer is, so the old strategy doesn't work; correct?

Mr. DECKER. The old strategy may not be as applicable today.

Mr. SHAYS. Would you walk me through—you have eight strategies, it seems to me, not—you have nine strategies not eight, unless I'm misreading it. And I would like to know—you have the National Security Strategy of the United States. Would you be able to articulate that in a fairly coherent way, as to what that is?

Mr. DECKER. Yes, sir. The National Security Strategy of the United States would be the top-most policy-driven piece that explains what's most important about this Nation's security from the international standpoint, from an economic standpoint, and from a democratic standpoint. It covers all those aspects of what has to be addressed to ensure our security for our way of life.

Mr. SHAYS. Now you blocked it out in the same size as the National Strategy for Homeland Security. Is it equal to or supersede the National Strategy for Homeland Security?

Mr. DECKER. Sir, that issue came—it's confusing to us based on our reading of the document, the Homeland Security Strategy, which states that the National Security Strategy and the National Homeland Security Strategy are mutually supporting documents and represent the top-most tier of the strategies. In contrast, our sense would be that there's only one National Security Strategy for the United States and that encompasses many issues, to include the threats we have from terrorism, and that the Homeland Security Strategy and the National Strategy for Combating Terrorism would be the two component pieces that deal with the problems of terrorism. And so our position is that it is confusing.

If it's confusing to us, and we happen to have done quite a bit of work on this, it might be confusing to other agencies, international partners, and so on as they start to look at specific goals and objectives.

Mr. SHAYS. Thank you.

Mr. Kucinich, we are going to do the 5-minute rule the first pass and 10 the second, and you have the floor.

Mr. KUCINICH. Thank you very much, Mr. Chairman.

Mr. Decker as you stated, there are perhaps 10 national strategies, more or less, each with overlapping and interrelated functions and each with a set of priorities. I'm concerned about the administration's conception of prioritization, however. The strategy has described many broad goals as priorities, but the strategies really don't involve any comparison. This is a priority, that's a priority, everything's a priority. But the process of prioritization means picking which comes first. It means choosing where the money will go. Is that not correct?

Mr. DECKER. Yes, sir. Strategy should help guide where you put resources against specific issues.

Mr. KUCINICH. Let me expand on this, if I may, and how they relate. Can you tell me, from the text of these national strategies, which is more important; for example, securing our ports or building missile defenses?

Mr. DECKER. Sir, I would like to answer that by saying that perhaps the priorities that are articulated in the National Security Strategy would be the big priorities for the Nation. But when you get below into the specific strategies with critical infrastructure protection, cyber issues, it gets a little bit more difficult to determine at that particular level which priorities are more important between the strategies.

Mr. KUCINICH. Let me help you, then. We know the administration is spending \$10 billion this year to defend the United States or to try to create a defense against a missile carrying a nuclear warhead, while spending less than a tenth of that amount to prevent nuclear material from entering our ports. Isn't that right?

Mr. DECKER. Sir, I'm not sure of the exact numbers.

Mr. KUCINICH. But you know they're trying to build a national missile defense on one hand and—there's a lot of money going to that—and on the other hand, there's concern about protecting the ports, and only a fraction of the money that is going to the national missile defense would be going toward the ports; is that correct?

Mr. DECKER. Yes, sir.

Mr. KUCINICH. Now at the same time, the Central Intelligence Agency reported in its recent national intelligence estimate that the threat of a national missile attack is actually less than that of an attack on our ports. Are you familiar with that public estimate?

Mr. DECKER. National intelligence estimate?

Mr. KUCINICH. Right.

Mr. DECKER. I'm familiar with some. I am not sure which one you're referring to.

Mr. KUCINICH. It's in the national intelligence estimate. The Central Intelligence Agency states that the threat of a missile attack is actually less than that of an attack at our ports. They're saying the ports may require more attention than building a missile defense that may or may not work 10 years from now. Do you have any comment on that in terms of priorities or how would you explain these anomalies?

Mr. DECKER. Sir, as we stated in previous testimony as well as the statement today, threat assessments should drive your policies and your strategies. At the national security strategy level, you look at all threats and you have to consider what they represent when you're trying to defend against them. My sense is that there are—not just the threat of terrorism, but there are other threats that the government has to address in different ways to ensure that we're prepared, that we can prevent if possible some of these threats, and, if we're not able to prevent them, to deal with the consequences.

Mr. KUCINICH. For example, the administration has not yet been able to make a case that Iraq represents an imminent threat to the United States, but there's a lot of money going into that, to a preemptive strike against Iraq; and on the other hand, there's not

money going for chemical and biological decontamination equipment to our hospitals.

In terms of priorities, what's your role in trying to be able to calibrate the priorities and compare one against the other to see if we're actually putting the money where it needs to be put in order to provide a measure of security for people in this country?

Mr. DECKER. Sir, we look at the strategies. We really do not critique the priorities per se. We have to assume that the government when they draft the strategy are using threat assessments and other tools to help them shape that strategy. And if they say that the strategy will have four goals or four priorities and here is the list of those priorities, we look at those in general way to ensure that do they make sense and is the rest of the implementation driven by those priorities.

Mr. KUCINICH. I want to thank the Chair and just point out that in connection with this discussion that the administration appears to be ready to spend about \$500 billion in Iraq, but so far there's only about \$36 billion that is being offered for securing our own country.

Mr. SHAYS. We'll have disagreements on numbers, but we'll proceed.

Here we go, Mr. Janklow.

Mr. KUCINICH. Thank you Mr. Chairman.

Mr. JANKLOW. Thank you very much, Mr. Chairman.

Mr. Decker, let me ask you, if I can, the National Strategy to Secure Cyberspace, the Money Laundering Strategy, the Strategy for Combat Weapons of Mass Destruction, the Strategy for Homeland Security, the Strategy Plan for the War on Terrorism, the Strategy for Combating Terrorism, the Strategy for Cyberspace, the Strategy for Physical Protection of Critical Infrastructure, and the National Security Strategy of the United States—that list that was prepared—do you know any of those that, standing alone, aren't important? You agree they're all important.

Mr. DECKER. Yes, sir. I think they have elements that are in a collective sense important.

Mr. JANKLOW. Am I correct, sir, that a part of your testimony was we're really not sure at this point in time that we have been able to effectively tie them all together into one comprehensive super-strategy, if I can call it that—I hate to keep using the word strategy—or policy or plan or whatever characterization you want to give; but we really haven't been able to effectively tie that into one set of documents yet, have we?

Mr. DECKER. Sir, if I can paraphrase. If we looked at these 10 strategies, albeit the National Drug Control Strategy is a very small piece—and this may not be the total list by the way, this is what we have come across—they represent a collage, if you will, on the government's attempt to deal with combating terrorism from a very broad look on the national level down to a more focused, when you are talking about money laundering or weapons of mass destruction.

Our sense is that because we haven't had time—some of these literally came out within the last couple of weeks, our sense is they may not all be wired and cross-walked or integrated in a way that, if you are that executive, in a Federal agency or a Governor or com-

pany or a CEO, that the pieces that really touch you, that you may have an important role, you may not be able to tease that out.

Mr. JANKLOW. Two other things. One, we can't minimize, I think, the whole question of drugs given the number of revelations that have been made over the past couple of years of the number of terrorist organizations that utilize drugs to raise money for their purposes. So clearly that has a role in this, No. 1. And, two, what are the institutional forces, what are the philosophical forces that prevent our country from sitting down and coming up with a master strategic plan that's debated and then becomes the plan, albeit it may be modified at times; but what's preventing us from coming up with a plan? Why do we have to keep issuing new documents. There isn't any human being that can follow all these.

Mr. DECKER. Sir, I would agree with you. The National Security Council, on behalf of the President, has responsibility to craft these strategies.

Mr. JANKLOW. What is your sense that is preventing this from happening? It can't be Republican-Democrat politics. Is it the bureaucracy or just our inability to understand it? What is it that's preventing this from happening?

Mr. DECKER. First, I think it's a pretty complex issue. And when you look at the partners that are involved, it makes it extremely hard to craft, when you talk about the role of the Federal Government, State, local, the private sector and the international, and some of that domain you control and some of it you do not control. And it becomes extremely hard when you're, say, with a task force that's charged to build a document that has the ability to accomplish—you know, to set clear goals and objectives that are achievable.

Mr. JANKLOW. It wasn't that hard during World War II after Pearl Harbor. Why is it so difficult now?

Mr. DECKER. Sir, I don't have a good answer for you. I think part of it may be if you look at the new Department of Homeland Security, the challenge that Governor Ridge is going to have blending 22 agencies, 170,000 people. I heard a comment that one of the major issues with some of the agencies was trying to determine perhaps what color uniform would be used by all.

Mr. JANKLOW. God bless America.

Mr. SHAYS. I thank the gentleman.

At this time, the Chair would recognize Congressman Bell from Texas.

Mr. BELL. Thank you very much, Mr. Chairman. I understand that the documents that you provided us today are intended, or I assume they're intended to offer a road map, if you will, from where we are trying to go in this area in the war against terrorism and overall national security. And in looking at the road map, a couple of questions come to mind, some of them were already touched on by my colleague, Mr. Kucinich, in terms of port security. And I think, and I want to be clear that you agree with the premise that—well, the suggestion has been made that a terrorist organization would be much more likely to smuggle a nuclear device into the United States via one of our ports rather than launching some kind of missile attack. Would you agree with that premise?

Mr. DECKER. Sir, I think the Intelligence Community and law enforcement community would probably agree with that, and I think that is more realistic.

Mr. BELL. And if you take that into consideration—and you didn't touch on specifics, but my understanding is that the budget proposal seeks over \$9 billion for missile defenses, while seeking less than \$1 billion for port security. And coming from Houston, TX, where we have the second largest port in the Nation, that's of obvious concern, and I am curious about the reason for that disconnect.

Mr. DECKER. Sir, I think the government tries to ensure that the priorities are set right and that the resources to work on those priorities is also linked. And this has to be driven by threat assessment. I don't have a reason, an answer to give you, why there's a difference between missile defense and port security. Why would there be a difference, you know, between first responder training issues, you know, and a vaccine? It's kind of like apples and oranges, if you will, and we are not privileged to understand some of the reasoning behind—

Mr. BELL. Let me interrupt, because it's not completely apples and oranges, because you all are setting the priorities. And if you already said that port security is a priority—and I realize there's not going to be a direct match-up in terms of dollars, but that's a pretty significant disparity when you're looking at \$9 billion compared to less than \$1 million, and really looking at the same kind of threat. I'm sure it is more expensive to develop missile defense systems, but that seems like a paltry sum to be spending on port security. And when you view a port like the Port of Houston, and travel the waterway and see what a daunting task it is to try and protect that amount of shoreline, it is obvious there's a tremendous amount of expense involved. And if the administration is not willing to make a more serious commitment to it, then it's just going to go unprotected.

Do you see any possibility for change or for it to be addressed further in the future?

Mr. DECKER. You addressed one of the key issues we stated before, in that there's going to be an awful lot of vulnerabilities. Governor Ridge, in his new responsibilities, is going to have to do a balancing act with the resources and the people to address the various concerns that he will be handling as the head of the Department of Homeland Security. Above him, the President is concerned about many threats and issues; and again, there's not enough funding, resources, or energy to cover all the vulnerabilities to this great Nation, so it comes down to making leadership decisions. Those have to be driven by information. Some of it perhaps we are privileged to know and see.

Mr. BELL. Can you touch on the coordination issue for just a moment as to who is going to be overseeing all of this, because that's a rather significant question as well.

Mr. DECKER. You're talking about the coordination—

Mr. BELL. Well, all of these various efforts that we have been presented with today.

Mr. DECKER. Sir, I suspect the newly formed committees of Congress will have direct oversight, particularly when you're talking

about homeland security. But when you deal with some of the more specific strategies, they touch a lot of different activities particularly here on the Hill.

The money laundering, I think the Banking Committee will be involved with aspects of that. When you talk about the National Military Strategic Plan for the War on Terrorism, the House and Senate Armed Services. Within the administration, this is—again, the oversight on whether these organizations are performing is probably going to be driven to a certain degree by the heads of the different agencies tasked to perform the duties under these different strategies. And the President and his team will have to determine are all the agencies and departments that are being tasked, are they coming together in a way that makes sense. And they will report this out, by the way, through their annual report to Congress on the results.

Mr. BELL. Thank you, Mr. Chairman.

Mr. SHAYS. It's not my attempt at all—I'm sorry, Mr. Murphy. Thank you very much, sir. We appreciate your service on this committee, and sorry I got so eager. I didn't want to leave you out.

Mr. MURPHY. I appreciate you noticing me.

Mr. SHAYS. You have an extra minute because I simply blew it.

Mr. MURPHY. You know, as I look upon this chart and as I read the many parts here, I'm reminded of the book and also now the movie, "Gods and Generals," which featured a lot of Stonewall Jackson, and he described his strategy with the enemy as "mystify, mislead and surprise."

I have to think in looking at this, any domestic and foreign enemies would look at this and they don't know how to make sense of this system, although I am sure it makes sense to someone, and I appreciate it has come out of a comprehensive look of setting many, many goals to combat terrorism.

But just a couple of questions and we can get into more specifics another time as to how this is done, but the key feature I see in this is communication. Can you describe to us how communication is set up between these strategies; for example, same agencies, different agencies, same people, different people? And I put that in the context of what we found in post-September 11th and as described by the folks up here, the difficulty in communicating between how many police forces did you say in this Nation—18,000 police forces, it's pretty massive—and how those strategies work at that communication to improve upon that?

Mr. DECKER. Sir, let me make a comment or two and then I would like to ask my colleague Steve Caldwell to address that. First off, most of the strategies are under the aegis of the National Security Council and many of the task forces, the working groups that were put together, and most—this is post-September 11th although several of these strategies are pre-existing before September 11th and have been readjusted to consider the impact of terrorism. Different working groups representing different agencies, departments, and sometimes it's the same person that may flow between some working groups—normally it's not—but there are some key members, participants that are the same. And they are given a charge, if you will, to work and build a particular document. Sometimes an agency will be given the lead for the document, pull-

ing in expertise from different agencies and departments as needed. So the partnerships that are developed on these working groups vary quite a bit depending upon the issue.

I'll ask Mr. Caldwell if he can provide a little bit more elaboration on that because some of these obviously are very tailored and some of them are very broad.

Mr. CALDWELL. Thank you. In terms of the coordination in general—and this will address one of the earlier questions as well—there's really two major mechanisms for coordinating here.

On the domestic side, you've got the Office of Homeland Security at the level above the individual agencies, you've got the Department of Homeland Security now, interagency working groups, and some of these interagency working groups actually work putting these plans together. And then you've got at the individual agency level lead agencies which then have other cases where agencies would support them, and in a few cases, for example, money laundering, there may be a little bit of confusion about who is the lead agency when you've got, say, Treasury and Justice both cited as leads in the National Money Laundering Strategy. And that's pretty much the domestic side.

On the overseas side you have the National Security Council, and within that you have interagency groups as well. For example, they had a specific interagency working group to come up with strategies here, the National Strategy for Combatting Terrorism. Then, again, you've got the lead agency concept.

Then you have the other partners, I'll call them. Those are within just the Federal family. The big challenges, as several of you have alluded to, on the domestic side is dealing with the State and local governments and the hundreds of fire departments just within a single State, as well as the 50 States and all of their subdivisions in the State and local level.

And then, of course, on the international side, you have the international community where you're dealing with other countries, you're dealing with international organizations and things like that.

Now, the key is to keep the international side of our coordination mechanism and our domestic side of the coordination mechanism talking to each other, and I think if you look at the two top-level strategies for both of those—actually, I think within the two plans there is a good deal of commonality.

For example, in what we'll call the overseas strategy, the National Strategy for Combatting Terrorism, there is an explicit objective to implement the other strategy, the National Strategy for Homeland Security. So I think those two strategies we look at as the top-level strategies, one being offensive and overseas, one being domestic and defensive under the top of the pyramid, as Mr. Decker said, which would be the National Security Strategy.

I'm sorry if our chart is a little bit mystifying. Hopefully the enemy finds it that way. But this is how the administration had portrayed those two strategies as being side by side, the National Security Strategy and the National Strategy for Homeland Security. But as Mr. Decker said, we see the National Strategy for Homeland Security as being maybe a coequal with the National

Strategy for Combatting Terrorism, one being offensive, one defensive; one domestic, one overseas.

And then the other strategies, a lot of them are really kind of functional strategies within that. So we do see some kind of hierarchy among these plans. Thank you.

Mr. MURPHY. Thank you, Mr. Chairman.

I yield back my time.

Mr. SHAYS. I want to just go through—and we're going to have a 10-minute cycle here. I'm not saying that Members don't have to use the 10 minutes, but I do want to make sure we cover some things, and if we cover them—and I know my colleagues may want to do that as well.

I want to ask you four basic questions that I want on the record that are part of your statement. I want to know what are the essential components of a successful national strategy. That is one of the questions I want. I want to know are these found within the eight Bush administration strategies to combat terrorism. So that is my first question.

Mr. DECKER. Sir, we would look for several key elements within a national level strategy. Obviously one of the most important things would be a vision, a mission statement, clear goals and objectives, roles and responsibilities delineated, a general scheme of how to accomplish some of this, and then some performance measurement issues so that you can measure your progress.

There also should be, when you talk about the mission and up in the vision statement, a sense of end state.

Mr. SHAYS. What—I'm not clear whether you have attempted to grade all of these eight strategies, and this is National Security Strategy, National Strategy for Combatting Terrorism, the homeland security, combatting weapons of mass destruction national strategy, the National Money Laundering Strategy, securing cyberspace, the physical protection of critical infrastructure. All of these, have you attempted to evaluate and give a grade of whether it meets the test of a good strategy?

Mr. DECKER. Sir, let me answer the question without grades. I would say some of the strategy documents are well written. They have most of the prerequisite pieces that we would expect, and this is for implementation purposes.

The National Strategy for Combatting Terrorism is very well written, has an excellent threat assessment linkage with why you're doing what you're trying to do.

Mr. SHAYS. I'm not going to ask you with my time to go through each one. I just want to know—

Mr. DECKER. Yes, sir. I was just going to give you the field goals, if you would.

Mr. SHAYS. OK. That is fair.

Mr. DECKER. The one that I think I would send back to redo or review would be the Strategy for Combatting Weapons of Mass Destruction. I believe it is only eight pages in length. It really doesn't do the issues that need to be done about the principles. It does talk about some focus areas and the roles and responsibilities. It is quite academic.

Mr. SHAYS. Have you seen—even those that are basically classified, you've gone through these strategies as well, correct?

Mr. DECKER. Yes, sir.

Mr. SHAYS. OK. I would like you to look at each one based on how you describe what a good strategy is, and I would like you to provide a document to this committee that we'll distribute to both sides, obviously, outlining on each of those tests how they measure up. OK?

Mr. DECKER. Yes, sir.

Mr. SHAYS. How will we know if the strategies are effective? I want to know what performance measures are planned to gauge the effectiveness of the strategies, and to what extent is the absence of a terrorist attack validation that our strategies have been successful?

Mr. DECKER. Sir, a strategy by itself, as I indicated, is just a document. It should have some pieces that would help guide the implementation. The performance measures to gauge the progress of whether you're succeeding against the war on terrorism by and large, are still under development.

We approach the performance and progress against the war on terrorism a little bit differently, and we would—we know how hard this is for people to wrestle with, but if you consider the war against terrorism or on terrorism much like the war on poverty, or the war on crime, you may never succeed in eliminating it totally. What you do have in the interim, you have positive operational events that lead to larger positive outcomes.

For instance, when you eliminate the leadership of a terrorist group, or you freeze their financial assets or you reduce the safe havens that they enjoy, you have accomplished quite a bit that will lead to an even greater outcome, which means perhaps less—fewer attacks of significant measure.

Mr. SHAYS. Thank you.

In regards to—I'm basically asking a question that relates to the first but are there aspects of combating terrorism that are overlooked or any holes in these strategies. I'm looking for the gaping ones, not the final ones, and you started to do it with one response, but when you look at these eight strategies, where do you see the holes?

Mr. DECKER. Sir, that links back into the review that we will do, looking at the integration to see where are those true fabrics. When I asked the team to take a look at that, we did not come up with any particular gap, except for the one on intelligence.

Mr. SHAYS. OK. How can the NSC, the National Security Council, more effectively coordinate the implementation and oversight of the eight national strategies? Is the Office of Homeland Security coordinating and implementing the national strategies? Those are my two questions. Do you want me to repeat them?

Mr. DECKER. Yes, sir, if you could paraphrase it just—

Mr. SHAYS. I want to know how can the NSC more effectively coordinate the implementation and oversight of the eight national strategies?

Mr. DECKER. Sir, I think the first step would be to better articulate how they all relate to each other and put it in a way that everyone—from the Secretary of the department down to a GS-7—can understand how they are in some type of precedence.

Mr. SHAYS. That's Congressman Janklow's basic concern.

Mr. DECKER. Sir, that would be No. 1. Then once that is done, then you have better success of trying to tease out whether some of the implementation is really being effective and efficient and how it's being done.

My sense is that—and my team, I give them a lot of credit—they looked at all the strategies. They talked to a lot of smart people, and they asked during one meeting at the senior level, has the executive branch come up with a schematic, a graphic depiction of this? And they said, it's too hard. They had not.

As far as we know, this is the only depiction of how these kind of hook together, and obviously it's not perfect, and it's very confusing.

Mr. SHAYS. Now, the one strategy that you added, your ninth strategy, is the National Military Strategy. So that's what you added there.

The one area—I think that Mr. Kucinich and I disagree on some statistics and numbers, and I happen to believe that preemptive is absolutely essential. I believe that Iraq represents an imminent threat, not something that's way off in the future. But the area where we do agree is that before September 11th we talked about what various commissions said, and particularly the Hart-Rudman said there needs to be a Department of Security. In that Department of Homeland Security, when I mentioned it to constituents before September 11th, they said, what are we, Great Britain? It seemed like a foreign thing.

Then September 11th happens. The President believes that he can deal with this issue with a coordinator. A lot of my Democratic colleagues and a few Republicans, and I was one of them, said we need something more significant, we need a Department of Homeland Security, and he ended up, I think, coming around to where most Democrats were.

But the one area that Mr. Kucinich and I think had some real problems was that while we knew we needed to reorganize, we never felt that the strategy—the threat was properly described. We think it was more on an intuitive response, and that the strategy was never fully described, and I want to be fair to Mr. Kucinich, but I think on these two issues, we thought that should happen. The difference is I felt we needed to get this Department moving, and I think this is still a work in progress.

So I'm happy we have a Department, but I am concerned that the administration didn't really state in a sufficient way what the threat was and what our strategy was to then begin this Department of Homeland Security.

I'm delighted you're here. I'll be recognizing other Members, and, Mr. Kucinich, I'll start with you.

Mr. KUCINICH. Thank you very much, Mr. Chairman.

National Security Strategy of the United States of America, homeland security, physical protection of critical infrastructure and key assets.

Sir, do you see the quandary which arises when preemption could actually be counterproductive to assuring the security of the United States of America, our home?

Mr. DECKER. Sir, I can only answer that the executive branch, the President has a lot of challenges he has to address, and these

strategies do address significant issues that the administration is trying to deal with.

Mr. KUCINICH. I'm going to read from the National Security Strategy: The United States has long maintained the action of preemptive actions to counter a sufficient threat to our national security. The greater the threat, the greater is the risk of inaction, and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack. To forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act preemptively.

I think to have this hearing without discussing Iraq would be inappropriate, because we are talking about a preemptive action against Iraq, and if the administration—and I'm happy to have any Member—I'll gladly yield to any Member who can articulate a case which says that Saddam Hussein has nuclear weapons, has biological and chemical weapons of mass destruction that are usable, has missiles with the potential to strike at this country, has the intention to do so, because I haven't seen anything on the public record which indicates a case for preemptive action, and yet the day before our vote on the Iraq resolution, the Central Intelligence Agency in a letter to Senator Graham indicated that there did not appear to be an intention on the part of Iraq to attack the United States. The New York Times last Sunday had a story that indicated that a preemptive attack on the part of the United States against Iraq could result in terrorism being visited upon our shores.

Mr. SHAYS. Would the gentleman like to yield? I'd be happy to jump—

Mr. KUCINICH. Sure, Mr. Chairman. I have a great respect for you, and I think that this would be an excellent opportunity for a colloquy on this, because I'm having trouble for understanding what the basis for preemptive action is.

Mr. SHAYS. Well, I think, frankly, it stems from a lot of the work in this committee. We know that Saddam Hussein had a viable chemical and biological program before the war in the Gulf. We didn't know that he had a viable nuclear program, but he did. We knew that he had a viable chemical and biological program after the war in the Gulf. We didn't know at the time that he had a nuclear program until we had a defector who came before this committee and told us that our intelligence community said there is no program and didn't accept his name or that he was in charge of it.

We then discovered where the nuclear program was when his two sons-in-law came to Jordan. They were debriefed. I spoke with one of the briefers. We were immediately able to send our colleagues the inspectors to those sites. They uncovered the nuclear program. So we had a clear one then. We destroyed the systems that he had, and then when we started to talk to the men and women who were making those chemical, biological, nuclear programs, Saddam became very belligerent. He started to threaten the inspectors, and we withdrew them. The fact is that he had one before the war, he had one after the war, and he kicked us out when we started to tear out the roots, not just destroy the weapon systems.

So I really think that the burden is on Saddam to explain to us what he did with those programs and what he did with the people. He hasn't done that, and section 1441 makes it very clear he needs to cooperate with the inspectors, and he needs to disarm. He has not done either the disarming or the cooperation.

Just to give you another example, just finding the empty canisters, the rockets that were empty, we had testimony in our committee that made a point that you don't load your weapon system with a chemical. You do it just before. Hans Blix pointed out they were in a new facility.

I could keep going. I don't know how much longer you want to yield to me, but our testimony before this committee was that we know he has a nuclear program. Our allies know he has a nuclear program. Our opponents know he has a nuclear program. The question is do we wait until he actually has the weapons-grade material? We had testimony before this committee that pointed out the weapons-grade material is the size of a softball if it is plutonium—excuse me, the size of a baseball if it is plutonium, the size of a softball—

Mr. KUCINICH. So you are saying based on that we should launch an attack against him?

Mr. SHAYS. No. I'm saying that he is within months potentially of getting nuclear weapons, and I don't even think Jimmy Carter would allow Saddam Hussein to have nuclear weapons. So your description to me is answered by that, but I could go on.

Mr. KUCINICH. Wait. But this is—and I appreciate the Chair being willing to engage in this colloquy, because we need to explore the ambiguities which exist. It is ambiguous that Saddam Hussein has nuclear capability right now. I think that actually it's less than ambiguous. He has no nuclear capability at this moment. According to information that has been made public from our own government, he's at least 10 years away from developing any nuclear capability. However, North Korea, North Korea at this very moment, North Korea is mentioned in a number of these security documents, and North Korea has the nuclear capability and is actually rattling a nuclear saber, yet no one is talking about a preemptive attack on North Korea.

Mr. SHAYS. There's a reason.

Mr. KUCINICH. Mr. Chairman, I think you're right, there is a reason, and the point is that if we are able to use diplomacy in dealing with North Korea, which has nuclear weapons, which is rattling a nuclear saber, we can do the same thing with Iraq which doesn't have nuclear weapons, even if they have a program that might not be viable for 10 years.

I want to add to this—

Mr. SHAYS. Could the gentleman just yield?

Mr. KUCINICH. Of course, Mr. Chairman. I think this is important that this debate take place.

Mr. SHAYS. Our CIA didn't even know he had a program and denied any program. It was not until we had a defector and his two sons-in-law pointed out that he had a very active program. It was—so your comment about the CIA suggesting or someone suggesting that 10 years away, we had testimony before our committee that

said it could be 6 months away. So, I mean, this very committee—

Mr. KUCINICH. Mr. Chairman, I would respectfully suggest that the Central Intelligence Agency, however its defects, is vastly more equipped to make an assessment of the capabilities of another government than would be a defector whose very presence in a committee room suggests that there's some political motive to his participation.

Now, I want to add this, and that is—and just for the record, I think that the Chair has made a case that inspections worked to destroy weapons, and that's actually what's going on right now. The inspections worked in the past to destroy Saddam Hussein's weaponmaking capability, and the U.N. inspectors are working to continue to do that right now. And all that I'm saying, Mr. Chairman, you know, with due respect, because I have the greatest respect for you, is that this doctrine of preemption, it doesn't appear that Iraq measures up to what would be the basis for preemptive action, that they haven't met that level, and on the other hand, North Korea presents a greater challenge, and I would not advocate a preemptive attack against North Korea, but I'd be less inclined to advocate one against Iraq, because it hasn't met the test, which would be the threshold of the national security doctrine of preemption.

And a final point here on this, and that is that inasmuch as the Federal Bureau of Investigation has had officials who have indicated a concern that an attack in Iraq would bring about terrorism to our shores, would create lone wolf attacks inside the United States, then we have to make an assessment whether this doctrine of national security runs actually—calling for preemption runs actually contrary to this doctrine which calls for homeland security.

And, Mr. Decker, it goes back to the earlier question I asked you, and that is we are prepared to spend—depending on the estimate—Lawrence Lindsey's estimate, \$200 billion, Professor Northouse of Yale, anywhere from \$99 billion to over \$1 trillion for a war against Iraq, a preemptive strike, occupation, reconstruction, all that money involved, and yet we're not devoting anywhere near the amount of money to secure our borders, our ports against the kind of attack which the FBI says is more likely if the United States launches a preemptive attack.

So do you have any comment on that? I mean, in your work, do you get a sense of proportion or priorities or anything like that, or are you just counting beans? What are you doing?

Mr. DECKER. Sir, I really can't comment on what you've just raised. I don't count beans. I look at issues, try to ensure that these strategies make sense in the implementation, and that they have the right component pieces to allow success.

Mr. KUCINICH. OK. Now, I raise this point, Mr. Chairman—I know my time is expired. I'll make it quick. You would think that these strategies would be integrated. I mean, I would think that's optimum, to have the strategies integrated. It would seem to me that an integrated strategy said that if you had to use preemption, that would then be in the defense of our home; however, if you see the possibility that the use of one strategy might run counter to another strategy, it's an opportunity for discussion.

I want to thank the Chair for engaging in this discussion. Thank you.

Mr. SHAYS. I thank the gentleman for his yielding to me.

At this time, Mr. Janklow, I'd love to ask if you would yield a second.

Mr. JANKLOW. Yes, sir.

Mr. SHAYS. Thank you.

Just to put on the record, we may be looking at the FBI data slightly differently. The FBI data that I've seen basically has said we will have terrorist attacks whether or not there is interaction with Iraq, and that potentially, if anything, they may just wait, but the attacks will still come.

We're not going to respond to the blackmail of Iraq, and I just wanted to make sure that I corrected for the record the number. I think it's very legitimate to raise some real questions about the amount of money that the military action will take, but the rebuilding of Iraq, it's very clear, the administration said will be spent on Iraqi oil for the Iraqi people. We are feeding them—the people have been starving; giving them medical help—the people hadn't been getting the medical help. And I just want to point out that expense, which will not be small, will be paid for by the 10 percent of the world's oil owned by the Iraqi people, just to make sure that's part of the record.

I thank the gentleman for yielding.

Mr. JANKLOW. Thank you, Mr. Chairman.

Mr. Chairman, other members of the committee, I hear people all the time using data to run figures around and the comment that there's some professor that thinks the war—a prospective war would cost \$1 trillion. That professor must be in the English department writing fiction and couldn't possibly be a person that understands anything about the current world events.

You know, some people make the suggestion that in the event that there were to be a war with Iraq, that America is going to be attacked by terrorists. I don't know what America did to become the recipients of the World Trade Center incidents. I clearly don't know what we did to precipitate the individual that was coming down from Canada that was apprehended at the border with the attempt to blow up things in our country. I don't know what we did to encourage the individual to get on the airplane and fly across the ocean with explosives in his shoes so he would try to blow up an airliner. I don't know what we did to precipitate the Cole incident where they blew up one of our ships in Yemen, but maybe someone could explain that to me at some point in time, and I won't be quite so ignorant on the subject as I apparently am right now.

But, Mr. Decker, if I can go back to questions with you, I'm really concerned about the fact that all these documents are well honed. People that sit and write them put a lot of thought and effort into them, but they do it in somewhat of an isolation within the sphere where they're working, and they're not looking at the big picture.

You know, it's going to be terribly difficult in this country to come up with an overall strategy, because of the nature of our Federal system, because of the nature of the way that this country is

structured and the division of responsibility and how we operate. In any State, the Governor thinks that he or she is the chief ultimate law enforcement official. The mayor of the city knows he or she is. The chief of police really knows it's in their department, until you talk to the sheriff who says, it's my jurisdiction, and the State's attorney says, no, you're all wrong, it's my jurisdiction. The county commission thinks that they have it, and we sit around complaining about the way the Federal agencies try and interact with each other.

Given the fact that these documents are drafted within the political system, where no matter what you do, someone is going to pick on you for not having done the right thing, for not having given the right emphasis to something, for not having given the right focus, wouldn't it be helpful if this was—there was legislation passed that basically mandated an overall document, if I could call it that, an overall strategy, that once it's prepared by the executive branch, then will be picked apart, critiqued and analyzed by the American people, by all of the various special interests, and by the Congress, so that we can respond to it, because the way we're doing it now, we're never—do you think we're ever going to bring it together into one structure, given the way our system operates?

I realize that's a compound question, but I think y'all—by the nodding of my head, you understand what I'm getting at, sir.

Mr. DECKER. Sir, let me break your question into two parts. One had to do with what legislation is needed, to pull this together to make sure it's integrated. The second part is whether this is mission impossible?

Regarding the first part, we've not done enough of the work that we have to look at—we know it's confusing, but where are the true gaps in the integration of all these strategies, and does it make sense to have one overarching national strategy to combat terrorism with key component pieces.

Mr. JANKLOW. Do you think it does?

Mr. DECKER. Well, I think what we did determine—I think there's a merit to having one strategy. However, if you look at that one strategy and break it in two parts, like Mr. Caldwell mentioned, you have a homeland security piece, and you have the overseas combating terrorism piece. They represent the domestic and international sections, if you will. Those two component pieces, in my view, could be very nicely crafted into one combating terrorism strategy with, obviously, the homeland security piece.

When you talk about money laundering, weapons of mass destruction, cyber and critical infrastructure protection and those issues, those are more functional, strategies that would dovetail into not just those two combating terrorism strategies, but perhaps even some larger issues. For instance, the cyber—protection of critical infrastructure and the cyber piece, you have threats that come from other countries, you know, not just from terrorist groups. So that has to be a broader strategy to deal with things that come out of the National Security Strategy.

When I talk about a pyramid, this is not a pyramid with nicely shaped, equal-sized boxes and blocks that would look really pretty. This might be, you know, a hybrid, if you will, of an Egyptian pyramid, a Mayan pyramid and some other type—

Mr. JANKLOW. But, sir, if we do that, if I can interrupt you for a minute, if we have all these different structures, how is anybody ever going to comprehend it? Who could pass the test on what it all says and what it all means? Who is going to figure it out?

Mr. DECKER. Well, that's why there's a crosswalk that hasn't happened, at least in our view, and that crosswalk, one of the indications we can tell—meaning has this document, this strategy, been linked into this other strategy—some of these key goals, objectives and references to this is a support piece for this other strategy, and we've only seen that in one or—you know, a couple of the strategy documents.

There was one revealing anecdote that my team mentioned. During an interview with a department, they were talking to a detailee from another major department that plays in combating terrorism, and the mention was, did you know about this strategy which came from the detailee's parent department. He had no idea that strategy was even being drafted.

Mr. JANKLOW. But isn't that always going to be the case the way we're doing it?

Mr. DECKER. Yes, sir.

Mr. JANKLOW. So we need another method. This one has proven to create a lot of nice documents, but they're not—they may be interrelated, but they're not coordinated, and if people are never going to figure it out—

Mr. DECKER. Well, I'll say they're not integrated. That's for sure. And if you have problems with integration with the documents, you're going to definitely have problems with coordination and—

Mr. JANKLOW. We talk about integrated working groups, integrating working groups. Just the mere fact that we've got to bring all these working groups together, you know, somebody once said that God so loved the world, He didn't send a committee, and this is what we're dealing with with all these interagency working groups all the time. When one member of the group quits and goes and gets another job, you've got to start all over again in bringing people up to speed.

Isn't there a better way to do it? When there was the old NATO and the new NATO, there was a Supreme Allied Commander. There was a person who was in charge. The military is a great model for this pyramid of getting things done, albeit they have difficulty dealing sometimes with the Army, Navy, Air Force and Marine Corps coordinating, far less today than they used to because the decision was made to really integrate these things into one operating sphere.

Please tell me, if you can, why can't this be done with our National Security Strategy as it pertains to terrorism?

Mr. DECKER. Sir, I think it can be done, and that's the role of leadership, the President, the National Security Adviser getting the team together and making sure that this constellation of strategies can be understood.

Mr. JANKLOW. Without bringing in ego, is this a job for the executive branch, or is it a job for the legislative branch?

Mr. DECKER. Well, I think legislation of some sort may be very useful in coming to closure on this issue. The actual degree, the mandating of what that language would be, I think I'd have to

think about that. The pressure, I mean, through our oversight, I mean, having someone from the executive branch explain why this cannot or is not being integrated or what would it take to integrate would be very useful.

Mr. SHAYS. I might say that the gentleman's time is up, but we certainly will make sure that the administration is, in fact, represented and testifies before the committee to point out how they're going to be integrating these; all of them being very important strategies, but how are they integrated? And I thank the gentleman for his questions.

At this time the Chair would recognize Mr. Bell for 10 minutes.

Mr. BELL. Thank you, Mr. Chairman.

I think I share some of my colleagues' frustration in that there does seem to be somewhat of a grab-bag approach to fighting the war on terrorism. It's everybody's responsibility, and then at the end of the day if something happens, where are we to look? Who is responsible?

And I want to take just one area, one of the strategies, and that is the National Strategy to Secure Cyberspace, because in looking at the document that was provided, the public-private partnership has suggested it will be again sort of everybody's responsibility, the Federal Government, the private sector, State governments, local officials. Who is going to be responsible for implementing the National Strategy to Secure Cyberspace?

Mr. DECKER. Sir, let me direct that question to Mr. Caldwell.

Mr. CALDWELL. Let me answer your question. In terms of the cyberspace, we have difficulties in a lot of these areas, because we've created a new department. There are incredible challenges ahead for this department, and the infrastructure protection is one of those responsibilities that has now shifted even within the Federal Government from the President's Critical Infrastructure Protection Board to a Cabinet-level department, and it has a division within there that would look at those kinds of issues.

And the problem that you were talking about in terms of the private partnerships, the partnerships with State and local governments as well, I mean, these are just things we're going to have to get used to in terms of the Federal system we live in, and the sovereignty and autonomy of our State governments, and the autonomy we give to the private sector, and rightly so. I don't think we want to change some of our basic precepts here in terms of what should be private and public in government and what shouldn't, because of these other things. I think that there are incentives, and government will use the normal incentives it always uses to try to get the private sector to do things, to do either taxation, revenue, subsidization, other types of partnership that—to try to get the government to—or the private sector to—

Mr. BELL. And that's fine. Let me interrupt, because that's all well and good, but at the end of the day somebody has to be responsible, and it needs to make sense, and it needs to be logical. And the area of cyberspace, if you're to believe the story in the Washington Post, and it appeared to be quite credible, that appeared several weeks ago, the Department of Defense is in the process of engaging in massive plans and having regular discussions about the ethics involved in cyberwarfare and mounting a

giant cyberwar effort, if you will. It seems that it would make sense that the Department of Defense would actually—or would also head up the effort to decide how to best guard against cyberwarfare in this country. Those who are developing the offense, it seems logical, would be in a pretty good position to also design a defense. Does that not make sense to you?

Mr. DECKER. Yes, sir, it does, and, in fact, I believe in the cyberdefense area, there are quite a few participants that are in the Federal area, some in the State, local, private. Some of the different institutions are involved. There are national security issues. There are criminal issues. There are terrorism issues. There are private citizen issues. I mean, there are a lot of participants in that.

One comment I would make with what Mr. Caldwell said about the strategy. When we looked at the strategy, there are some things that are directed, and then there are some things that are hoped, that are less—more of a voluntary nature, and my sense is that when you're dealing with Federal, State, local, private sector, international partners, it's a very delicate walk between what you can direct and what you hope will be the outcome of voluntary participation. I think that's one of the challenges with the critical infrastructure piece and the cyber piece is people have to be willing to agree with your strategy and maybe the investment in those areas that they have to allow for this comprehensive security framework. That's going to be the real big challenge.

I heard this when I was out in California last year, talking to an audience of people that were involved with the port authority at Los Angeles and Long Beach. The issue was how much funding was the Federal Government going to give to help on port security. There were partners in there from the union, from private owners, from the State, local, the Federal Government. What came out of the private sector was, you know, when we need to fix the security here, we're also going to need to fix a lot of the infrastructure issues, because these ports were built back in World War II-era, and the ships can't get close enough. There are a lot of issues.

So it's very complicated when you're asking people to put investment in for, in this case, security, be it cyber or physical infrastructure, and there's other ramifications on that investment, and it's very difficult for a lot of entities outside the Federal Government to know exactly what to do.

Mr. BELL. While there's still time, I want to touch on one other area that I consider quite important. Obviously, as the Chair pointed out, I'm a freshman member, so I've just been here a couple months. Most of the focus has been on Iraq. A tremendous amount of the focus has been on international terrorism, and I've always felt that we have a very reactive government, and we tend to adopt this mindset that yesterday's problem mattered yesterday. Now we need to move on to today's problem and tomorrow's problem, forgetting that yesterday's problem can very easily creep back and become today's problem. And not too many years ago back in 1995, 1996, the major threat to many people or many people considered one of the major threats on the terrorism front to be domestic terrorism, fringe groups within our own borders.

Now, as I said, I've been here 2 months, and I've heard no talk about domestic terrorism whatsoever or any efforts to infiltrate and to make sure that those types of extremist groups are not going to be creeping back into the forefront and doing the kind of damage that we saw in Oklahoma City several years back. I'm curious, have we moved on? Are we just focusing on international tier and threats from abroad? I understand obviously there will be some overlap in these efforts that would not only be effective against international terrorists, but would also be effective against those types of efforts within our own borders, but it does seem that an overwhelming amount of the concentration is on terrorists abroad, and I'm curious as to what that's doing to our focus here at home, if you could comment on that.

Mr. DECKER. Sir, recently the FBI has released a national threat assessment, which we have asked for and the committee has requested that this be done as well going back to 1999, and we've not had a chance to review it in its totality, but if it's a good threat assessment, it should have the domestic whether they are the home-grown variety or farm variety threat, be it from terrorism, in that document. My understanding is that it is a classified document, and there's two versions, but there's a law enforcement sensitive. We plan to review that document to better understand is it a comprehensive assessment.

Mr. BELL. Just to humor us, if you all could start including some of these domestic efforts in these overall plans, that would be great.

Mr. DECKER. Sir.

Mr. BELL. Thank you.

Thank you, Mr. Chairman.

Mr. SHAYS. Thank you very much, Congressman Bell.

We are joined by Mr. Turner, who is the vice chairman of the committee, and it's kind of interesting for me to think that one of our Members is a former Governor and had that kind of chief executive approach to his questions. And Mr. Turner is the chief executive in Dayton and helped balance budgets, and we're just delighted that you're the vice chair of the committee and just would recognize you. And I think your wish is that we get on to the next panel; is that correct?

I would just note for the record that last week we had—this committee did have a briefing by the FBI on the threat assessment of the FBI, and one of the challenges we have is that—and I say this to you, Mr. Bell—is that it is basically a classified document. It's not something the press can talk about. But while some people are focused on Iraq and some in Korea, we've got some who couldn't tell you anything about Iraq or Korea, but can tell you a lot about the threat assessment that we're dealing with domestically. A lot has happened. It's pretty impressive.

At this time I thank you, Mr. Decker and Mr. Caldwell. I think the highlight for me was the question to you on the cyberspace stuff, and I thank both of you for your very fine answers and for the committee's participation. We've been keeping the other panel waiting a bit longer than I thought, but it's been very interesting having you both testify.

At this time we will go to the next panel. Is there anything I guess I should have said, Mr. Decker, that you want to put on the record before we go?

Mr. DECKER. Yes, sir, if I could make one comment. I would hope in a year from now when this issue is revisited, that it will have been totally sorted out so that we are on an effective path for implementation.

Mr. SHAYS. Guess what? We're going to have you here in 6 months, and we're going to hope in 6 months it's done. Is that a deal?

Mr. DECKER. Yes, sir.

Mr. SHAYS. And you guys will be pushing the administration, and we will, and we're kind of the catalyst, and they'll do their job, too.

Mr. DECKER. Thank you.

Mr. SHAYS. Thank you very much.

At this time the Chair will announce the second panel. Our second panel is the Honorable James Gilmore III, former Governor of Virginia; chairman, Advisory Panel to Assess the Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. That's why we call it the Gilmore Commission. I think if you want to have a commission named after yourself, you just give it a long title, and then they just decide to use the chairman's name.

We have Dr. Michael O' Hanlon, senior fellow, Foreign Policy Studies, the Sydney Stein, Jr. Chair, the Brookings Institution.

We have Dr. Andrew Krepinevich, executive director of Center for Strategic and Budgetary Assessment; and Mr. John Newhouse, senior fellow, Center for Defense Information.

I welcome all four to the panel. I'm going to have you stand up, and stay standing, because I'm going to swear you guys in. If you'd raise your right hands.

[Witnesses sworn.]

Mr. SHAYS. Thank you. We'll note for the record a response in the affirmative.

Mr. Newhouse, I'm going to have you move your chair over a little slightly.

Dr. O'Hanlon, you can move yours over slightly, too.

OK. We're changing the batting order a bit. We're going to have Governor Gilmore speak first, and then, Dr. O'Hanlon, you'll be second. Mr. Newhouse, we're going to have you third, and we're going to have Mr. Krepinevich be the cleanup batter here.

Let me say to you first, Governor Gilmore, you have been before our committee on a number of occasions, and if it hasn't been you, it's been someone else on the Gilmore Commission, and we appreciate what you did before September 11th, and we appreciate what you're doing now. I have read the testimony that was submitted that was available to me last night, and this is an excellent panel. We're really delighted you all are here. Looking forward to what you'll have to say.

Mr. GILMORE. Mr. Chairman, thank you very much—

Mr. SHAYS. I'm going to have you turn that mic on. Let me just do what I said before and ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in

the record, and that the record remain open for 3 days for that purpose, and without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted to include their written statements in the record. Without objection, so ordered.

I would say to the witnesses that if you want to touch on any of the questions that you've heard, we forced you to listen to the first panel but if there are some points that you think need to be addressed, feel free to do that. Regretfully, some of your statements are even longer than 10 minutes, so I know you'll have to summarize, so we welcome that, but your statements were excellent.

Sorry for the interruption. We'll start all over again, Governor.

STATEMENTS OF JAMES S. GILMORE III, CHAIRMAN, ADVISORY PANEL TO ASSESS THE DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION; MICHAEL E. O'HANLON, SENIOR FELLOW, FOREIGN POLICY STUDIES, THE SYDNEY STEIN, JR. CHAIR, THE BROOKINGS INSTITUTION; JOHN NEWHOUSE, SENIOR FELLOW, CENTER FOR DEFENSE INFORMATION; AND ANDREW F. KREPINEVICH, EXECUTIVE DIRECTOR, CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS

Mr. GILMORE. Mr. Chairman, thank you very much, and I will summarize, I believe, within the timeframe, maybe offer one or two additional thoughts than are contained within the written presentation.

Mr. Chairman, I'm pleased to be here with you and with the others—not only with the other Members of Congress. Thank you very much, gentlemen, for the chance to be here with you, and particularly my former colleague Governor Janklow, who is an old pal of mine. So nice to see you, Governor—Congressman.

Ladies and gentlemen, the September 11th, of course, has changed everything. It seems to me like that much of what we are doing and what we're thinking about and the way we're evolving as a Nation is simply being driven by the September 11th attack. It certainly was traumatic and continues, in my judgment, to be traumatic to this day, and as a result we're dealing with issues we previously have not dealt with, and we may even deal with them in ways that we probably—would be different than the previous time.

Our reports—as you know, we have now four reports. We are the official advisory body to the U.S. Congress. We were established through the House of Representatives. Congressman Curt Weldon, I think, initiated it. The Congress passed it. The Senate did as well, and we're your official panel.

The Commission was accomplished in January 1999. At that time there was no public commission involving this kind of issue. We began to go to work on it. In the first year, in a somewhat academic way, we established a threat assessment. We called it a national strategy. We, I believe, appropriately assessed the threat, and our most recent discussions have confirmed all that.

The second year we did major policy work, recommending an Office of Homeland Security; recommending the formation of a national strategy; focusing on the Federal, State and local involve-

ment, not just Federal involvement; focusing on the difficulty of intelligence stovepiping; and beginning to establish, I think, the framework for debate. That was presented to the Congress and to the President in December 2000.

In the year 2001 we focused on some major primary areas and began to get ready to go to business on our 3-year Commission when the September 11th attack occurred. This Congress then in its wisdom extended our Commission 2 more years.

We have now completed our fourth Commission report. I believe each of you has a copy of this report that has been delivered to your offices. We are now beginning our 5th year of—the 2-year extension for our 5th year of the Commission.

What are my opening remarks? No. 1, things have gotten a lot better because we do have these strategies. I think that the committee here is doing a real service to the Congress, to the public, by focusing on the plethora of the different groups of strategies and how they interrelate with each other and how that bears upon our national security. But at least we have strategies. We have the topics being laid out. That is a judgment call in itself in key and important areas. It looks to me like we're in large measure dealing with the correct types of issues.

Our panel in its 3rd year focused our attention on the value and the focus of State and local involvement within the national strategy and how you engage State and local people; a major portion on health care, which has been a primary focus of our Commission through all of its 4 years, the importance of health care in the health care system; the importance of border controls and beginning to watch people going in and out and maybe protect our borders in an appropriate way; the appropriate use of the military, a very profound issue at this time as we begin to key up the U.S. military to operate within the homeland, an extremely sensitive and important policy area; and cyberterrorism. These are the areas that we focused on.

What are the national strategies focused on at this point? There's an overarching strategy for the defense of the United States of a geopolitical position. There is a strategy to counter terrorism; a military plan to operate overseas in order to interdict and disrupt people who would attack us from foreign countries; a homeland security strategy; specific areas of weapons of mass destruction, a strategy for that; money laundering in order to break up the finance for people who would conduct these kind of military operations such as those we saw on September 11th; a cyberterrorism strategy; and a critical infrastructure protection strategy.

This is similar to the types of issues that we laid in over the last 4 years. And all of the topics are beginning in a rough way to come together in the appropriate ways. The trick, it seems to me, is to strive for focus in order to make sure that we come together to do the right things. I think one of the earlier speakers said that we need to get to the proper end state, and indeed we do. We need to focus on what we are trying to get to with these proper strategies, not just simply saying that the Nation shall be more secure, homeland shall be more secure. What are we looking to achieve here? What is the ultimate goal of all of these strategies?

One key, of course, is to continue to tie in the State and the local authorities. Federal strategy alone will not do that, although most of these strategies, I think, do make reference to the role of States and locals within the respective strategies, and that is certainly a positive point. But the truth of the matter is that you have to have a national strategy, not a Federal strategy, and that means that Governors and key mayors and key law enforcement officials all across the 50 States have to be tied in and included within an overall national strategy. We have to determine from their point of view what they need in their respective States, how it develops into a statewide program, how that interacts with their localities, what kinds of equipment and processes are needed in order to support that kind of strategy, how does the Federal Government play that kind of role, how do you develop the joint types of fundings, and then how finally do you get into exercising and then measure the results of what that end state is to be.

So, therefore, there has to be a complete focus on State and local and with the Federal partnership, and that is the end state that our Commission has focused on for several years.

And then I think we have to ask ourselves at the end, what is the goal that we are trying to achieve here? Is absolute security an obtainable goal? Is it attainable? Historically the answer is probably no. This is not a unique time that we face here today, although the violence of the September 11th attack has created a trauma that only replicates itself several times in American history. But we have seen the previous assassination of President McKinley, and then so shortly thereafter, only a few years later, the shooting of Theodore Roosevelt at a political event, the shooting and killing of President Lincoln. One might argue that was, in fact, a terrorist attack in and of itself here in the homeland, the Oklahoma City bombing, a domestic catastrophe of tremendous proportions, lead up of other areas as well. But this is not necessarily a unique time, but we now have to gain the perspective to make sure that as we react to it and we put together our strategies and programs, that we remember the longstanding values that we have as Americans, and that we don't impinge upon any of those.

And that primarily, of course, leads me back to the theme that we very frequently stress, and that is the civil liberties of the American people.

It would be so easy to strive for absolute security and to try to persuade the American people that we are going to reach for absolute security and to ask them to surrender all their civil liberties in order to attain that end. Our Commission believes that would be the wrong approach, and that the goal here must be to gain the maximum possible security within this country and then to tell the American people in a straightforward and honest way that total and absolute security is not possible; to get to the maximum level of security we can reasonably do consistent with the values and safety of the people of the United States, naturally spending a great deal of focus on weapons of mass destruction, because that would be the most terrible possible violation of the security that we might have; but within all those goals, that we believe that the eight strategies are a step in the right direction.

We congratulate this committee for going about the oversight work now of determining how the eight could be harmonized best together and work together for the national security, but I urge you to think closely about the value of making sure the States and the locals are contained within the national strategy.

Mr. SHAYS. Thank you, Governor. It's a nice way to start this panel. I had forgotten that Curt Weldon had led the charge on this. He has been one of the heroes, I think, on the issue of terrorism well before September 11th, and I'm not sure he gets the credit he deserves. He gets a lot of credit, but I think he deserves more.

Thank you.

[The prepared statement of Mr. Gilmore follows:]

**Testimony of
James S. Gilmore, III
Chairman,
Advisory Panel to Assess Domestic Response Capabilities
for Terrorism Involving Weapons of Mass Destruction**

**Before the
Subcommittee on National Security, Emerging Threats, and
International Relations
Committee on Government Reform
U.S. House of Representatives**

March 3, 2003

Mister Chairman, Ranking Member, and Members of the Subcommittee, I am honored to be here today. I come before you as the Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. 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 105-261 (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.

That Act required 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 three times during the course of the Advisory Panel's deliberations—on December 15 in 1999, 2000, and 2001.

The Advisory Panel's tenure was extended for two years in accordance with Section 1514 of the National Defense Authorization Act for Fiscal Year 2002 (S. 1358, Public Law 107-107, 107th Congress, First Session), which was signed into law by the President on December 28, 2001. By virtue of that legislation, the panel was required to submit two additional reports—one on December 15 of 2002, and one on December 15 of this year.

Leadership of the Subcommittee

Let me commend this panel, and especially its Chairman, for your continuing leadership in bringing these issues involving homeland security and combating terrorism before the U.S. Congress and the American people.

Advisory Panel Composition

Mr. Chairman, as I usually do on occasions like this, please allow me to pay special tribute to the men and women who serve on our panel.

This Advisory Panel is unique in one very important way. It is not the typical national "blue ribbon" panel, which in most cases historically have been composed almost exclusively of what I will refer to as "Washington Insiders"—people who have spent most of their professional careers inside the Beltway. This panel has a sprinkling of that kind of

experience—a former Member of Congress and Secretary of the Army, a former State Department Ambassador-at-Large for Counterterrorism, a former senior executive from the CIA and the FBI, a former senior member of the Intelligence Community, the former head of a national academy on public health, two retired flag-rank military officers, a former senior executive in a non-governmental charitable organization, and the head of a national law enforcement foundation. But what truly makes this panel special and, therefore, causes its pronouncement to carry significantly more weight, is the contribution from the members of the panel from the rest of the country:

- Three directors of state emergency management agencies, from California, Iowa, and Indiana, two of whom now also serve their Governor's as Homeland Security Advisors
- The deputy director of a state homeland security agency
- A state epidemiologist and director of a state public health agency
- A former city manager of a mid-size city
- The chief of police of a suburban city in a major metropolitan area
- Senior professional and volunteer fire fighters
- A senior emergency medical services officer of a major metropolitan area
- And, of course—in the person of your witness—a former State governor

These are representatives of the true “first responders”—those heroic men and women who put their lives on the line every day for the public health and safety of all Americans.

Moreover, so many of these panel members are also national leaders in their professions: our EMS member is a past president of the national association of emergency medical technicians; one of our emergency managers is the past president of her national association; our law officer now is president of the international association of chiefs of police; our epidemiologist is past president of her professional organization; one of our local firefighters is chair of the terrorism committee of the international association of fire chiefs; the other is chair of the prestigious national Interagency Board for Equipment Standardization and InterOperability.

Read our reports and you will understand what that expertise has meant to the policy recommendations that we have made, especially for the events of last year.

Those attacks continue to carry much poignancy for us, because of the direct loss to the panel. Ray Downey, Department Deputy Chief and chief-in-charge of Special Operations Command, Fire Department of the City of New York, known to this subcommittee and others like it throughout the Congress, perished in the attack on the New York World Trade Center. Although we continue to miss Ray's superb advice, counsel, and dedication to these issues, we trust that Ray knows that we are carrying on in the tradition that he helped us establish.

Our Continuing Mission

Mr. Chairman and Members, this Advisory Panel continues to work hard to develop the best possible policy recommendations for consideration by the President and the Congress. Now, of course, people and organizations are coming out of the woodwork, claiming to be all manner of "experts" in homeland security. At the same time, this panel is toiling away, seeking neither fame nor credit for its work, simply trying to find some rational and feasible solutions to many problems and challenges that still face us.

Observations about Terrorism Preparedness

In the course of our deliberations, the Advisory Panel has been guided by several basic observations and assumptions that have helped to inform our conclusions and policy recommendations for improving our preparedness to combat terrorism.

First, all terrorism is "local," or at least will start locally. That fact has a lot to do, in our view, with the emphasis, the priorities, and the allocation of resources to address requirements. September 11 and the subsequent anthrax attacks were further proof of that basic assumption.

Second, a major attack anywhere inside our borders will likely be beyond the response capabilities of a local jurisdiction, and will, therefore, require outside help—perhaps from other local jurisdictions, from that jurisdiction’s state government or multiple state resources, perhaps from the Federal government, if the attack is significant enough to exhaust other resources. That principle was likewise validated last September.

Given those two factors, our approach to combating terrorism should be from the “bottom up”—with the requirements of State and local response entities foremost in mind.

We note that we have many existing capabilities that we can build on in an “all-hazards” approach, which can include capabilities for combating terrorism.

Our thorough research and deliberations have also led us to observe that there is great apprehension among States and localities that some Federal entity will attempt to come in and take charge of all activities and displace local response efforts and expertise. That was not and likely could not, because of the actual circumstances in New York, have been the case in September. But all events may not unfold in that fashion.

Based on a significant amount of analysis and discussion, we have been of the view that few if any major structural or legal changes are required to improve our collective efforts; and that the “first order” challenges are policy and better organization—not simply more money or new technology.

With respect to Federal efforts, more than two years ago we concluded that, prior to an actual event, no one cabinet department or agency can “supervise” the efforts of other federal departments or agencies. When an event occurs, response will be situational dependent; federal agencies can execute responsibilities within existing authority and expertise, but under established “Lead Federal Agency” coordinating processes.

Support for Panel Activities and Reports

Mr. Chairman, the enabling legislation directed that analytical and other support for the Advisory Panel would be provided by a Federally Funded Research and Development Center. We have been exceptionally fortunate to have that support provided by The RAND Corporation. The breadth and depth of experience at RAND in terrorism and policy issues across a broad spectrum have made possible the panel's success in accomplishing its mandate. Its assessments of federal programs, its case studies and hundreds of interviews across the country and around the world, its seminal work in surveying state and local response entities nationwide, its facilitation of our discussion—leading to near unanimity of members on this broad spectrum of recommendations, its work in drafting reports based on our extensive deliberations, all have combined to make this effort a most effective and meaningful one.

Issues of Interest to the Subcommittee

Mr. Chairman and Members, I intend to outline for the record later in my testimony the key policy recommendations made by the Advisory Panel in each four reports to the President and the Congress.

Before I do that, let me address the specific questions posed by the subcommittee in your letter of invitation. You have asked that I comment on a number of the national strategies promulgated by the Bush Administration in recent months. Given both the nature and the timing of the release of those strategies, the Advisory Panel has only addressed one of those in any detail—*The National Strategy for Homeland Security*, released by the White House last July.

We commented on that *National Strategy* in some detail in our Fourth Report to the President and the Congress, dated December 15, 2002. We made both general comments and also addressed specific issues within each chapter. Here is what we said:

ASSESSING THE NATIONAL STRATEGY FOR HOMELAND SECURITY

The capstone recommendation in our *Second Report* was the need for a comprehensive, coherent, functional national strategy: “The President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office.” In that report, we described, in considerable detail, our proposed framework for that strategy.

In July of 2003, the President approved for release the first *National Strategy for Homeland Security*.¹ To lay the groundwork for most of the recommendations in the chapter of our fourth report entitled “Organizing the National Effort,” we start with a commentary on that *National Strategy* from the panel’s perspective, for the most part tracking the subject headings of the chapters on “critical mission areas” in that document.

General Comments

We applaud the President and his staff for publishing this comprehensive vision to serve as the framework for the entire national effort. It is a foundation document and an important first step. It should not—indeed it cannot—be seen as being all of the answers to the challenges that we face. It will require periodic updates: we suggest annually. It will require detailed implementation plans; some are already being developed.

It contains well-crafted “vision” statements of where we should be headed as a nation. It acknowledges—as we have said before that any comprehensive strategy must—that there are significant international implications for “domestic” efforts.

It recognizes that this strategic approach must be a truly *national*, not just a Federal approach:

... based on the principles of shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people. The National Strategy for Homeland Security belongs and applies to the Nation as a whole, not just

¹ *National Strategy for Homeland Security*, available at <http://www.whitehouse.gov/homeland/book/index.html>, last accessed December 5, 2002, hereinafter the “*National Strategy*.”

to the President's proposed Department of Homeland Security or the federal government.

It contains—importantly—definitions of both *homeland security* and *terrorism*:

Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

The National Strategy for Homeland Security characterizes terrorism as any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments.

It contains language about the importance of measures of performance but does not articulate what those measures should be. Importantly, in our view—being consistent with our expressions since our *First Report*—it eliminates the arbitrary, artificial, and confusing distinction between so-called “crisis management” and “consequence management” activities.

It recognizes the importance of creating a national incident management system with an “all-hazards” approach—one that combines preparedness and response for natural disasters, accidents, and intentionally perpetrated attacks.

Definitional Issues

Despite a commendable attempt to reduce confusion by articulating certain definitions, it does not fully accomplish the task. The *National Strategy* uses CBRN or CBRNE and Weapons of Mass Destruction or WMD seemingly interchangeably.

It uses different terms apparently to describe the same function or category: “health,” “public health,” “medical,” “medical care.” And it is unclear whether “emergency medical providers” does or does not include emergency medical technicians. It uses other terms interchangeably with not clear delineation or distinction: “anti-terrorism,” “counterterrorism,” and “combating terrorism.” And it is not clear whether “enemies” and “terrorists” are synonymous.

“Threat and Vulnerability” Chapter

This chapter of the *National Strategy* appropriately recognizes that the nature of our society—our “American way of life”—makes us inherently vulnerable to terrorist attacks. It also acknowledges the imperatives not only of safeguarding our security and economy but also our culture, our civil liberties, democracy itself.

It appropriately, in our view, disaggregates chemical, biological, radiological, nuclear, conventional, and cyber attacks. But it suggests that chemical and biological weapons, generically, are “easy to manufacture,” using “basic equipment.” We have noted, in our threat assessments, including the one in the Fourth Report, that such broad categorizations are unfortunate. Many of the more sophisticated chemical and biological weapons, especially those that could cause fatalities in the thousands or tens of thousands are very difficult to produce, maintain, and deliver.

It appropriately recognizes the potential damage that could result from an attack on U.S. agriculture.

“Organizing for a Secure Homeland” Chapter

This chapter of the *National Strategy* recognizes and explains the interconnected and interdependent roles of the Federal government, States and localities, the private sector, and the American people in a united national effort. It stresses the “vital need for cooperation between the Federal government and State and local governments . . . horizontally (within each level of government) and vertically (among various levels of government).”

In a move that we strongly endorse, it announces the intention to retain the White House Office of Homeland Security, even after the formation of the new Department of Homeland Security, with authority “to certify that the budgets of . . . executive branch departments will enable them to carry out their homeland security responsibilities.”

It appropriately notes that the Department of Defense has important roles in homeland security, both for “homeland defense”—“military missions such as combat air patrols or maritime defense” in which the Department would “take the lead in defending the people and territory of our country—as well as “military support to civil authorities”—where the Department supports other agencies in responding to attacks, natural disasters, or “other catastrophes.”

It appropriately, we believe, calls on the Governors of the several States “to establish a single Homeland Security Task Force (HSTF) for the state, to serve as his or her primary coordinating body with the federal government,” but unfortunately does not offer to do the same in return. (We address this issue directly later in the Fourth Report, as you will see in my testimony below.)

“Intelligence and Warning” Chapter

This chapter correctly notes that appropriate assessments—both “tactical” and strategic”—of terrorist threats must precede any realistic assessment of our vulnerability. We are arguably infinitely vulnerable. Only when we can realistically determine what threats exist that would seek to exploit particular vulnerabilities will we be in position to take preventive and defensive steps and other appropriate responses.

Unfortunately, the *Strategy* does not suggest what products of the tactical or strategic (especially strategic) assessments will be produced or how and to whom such products will be disseminated.

We address, in considerable detail, the issues of intelligence collection, analysis, and dissemination and make specific policy recommendations with respect thereto in our Fourth Report, which are outlined later in this testimony.

“Border and Transportation Security” Chapter

That chapter clearly and appropriately sets forth important initiatives for improving security at our borders and in our transportation systems. It notes the potential for using biometrics for improved identification, the criticality of deploying a border “entry-exit” system for foreign visitors, for increasing security with respect to commercial cargo entering the United States, for implementing “unified, national standards” for transportation security, for providing additional resources for the U.S. Coast Guard, and for improving visa processes.

On the latter issue, it suggests that the new Department of Homeland Security will “control the issuance of visas to foreigners” but provides no detail on how that will be accomplished.

“Domestic Counterterrorism” Chapter

Near the beginning of that chapter of the *National Strategy* is an explicit statement:

The U.S. government has not yet developed a satisfactory system to analyze information in order to predict and assess the threat of a terrorist attack within the United States.

We fully concur and offer a specific recommendation in our Fourth Report directed at helping to solve that problem.

While discussing several tactical and operational approaches to address the challenges in this arena, this chapter does not, in our view, address some of the more strategic issues, such as the important relationship between the Department of Justice and the Department of Homeland Security and the critical role that State and local law enforcement have in this area. It also does nothing to address the proliferation of interagency and intergovernmental mechanisms, which seem not to be part of any overall design. We address that issue below, as well.

“Protecting Critical Infrastructures and Key Assets” Chapter

We applaud the policy decision, articulated in this chapter, to “unify the responsibility for coordinating cyber and physical infrastructure protection efforts” into the new DHS, especially for providing a single point of contact on such issues for States, localities, and the private sector.

The chapter also notes the intention to create a national infrastructure protection plan—a laudable goal—as well as the recognition of the international interdependencies of many critical infrastructures, especially in the transportation and cyber realms.

We also note with approval the careful articulation of Lead Agency responsibilities for critical infrastructure protection. We believe that that model should be applied to other functional areas for combating terrorisms and cite specific instances of that in other parts of our Forth Report.

“Defending Against Catastrophic Threats” Chapter

We concur in the initiatives in this chapter for specific improvements in sensors and other detection and health surveillance capabilities. Those initiatives are fully consistent with specific recommendations contained in earlier reports of our panel.

The chapter acknowledges the need for improvements in laboratory capabilities but does not articulate specific proposals to address that issue. We do so, along with other policy recommendations, in our health and medical chapter later in this report.

“Emergency Preparedness and Response” Chapter

We concur strongly in the views expressed in the chapter on the different, separate response plans. We agree (as we have consistently expressed) that such plans should be merged. That chapter calls that proposed plan the “Federal Incident Management Plan.” We suggest that the better title would be *National Incident Response Plan*, which by its name would recognize the important role of

States, localities, and the private sector. The accompanying proposal to establish a national incident management system certainly recognizes that, and the name of the plan should as well.

We wholeheartedly endorse the intention to develop a "national emergency communications plan" designed to establish "protocols, processes, and national standards for technology acquisition." We have previously recommended such a process for all emergency response equipment and systems. It is especially critical in the area of communications.

We also applaud the emphasis in that chapter of the *National Strategy* of improving both coordination with and the capabilities of the public health sector. We have previously made recommendations in this area, and make additional ones in our Fourth Report, in our chapter on health and medical issues.

On the issue of military support to civil authorities, the parameters of which are outlined in this chapter of the *Strategy*, we devote a considerable amount in our Fourth Report, with several specific policy recommendations, outlined later.

THE NATIONAL STRATEGY FOR COMBATING TERRORISM

Mr. Chairman, the Advisory Panel has not had an opportunity to discuss and comment on this *Strategy*, given the fact that it was only released a few days ago. We will, however, undertake to do that in our next report to the President and the Congress, due later this year.

Our Reports

In our first three reports, the advisory panel has, through its assessments and recommendations, laid a firm foundation for actions that must be taken across a broad spectrum of threats in a number of strategic and functional contexts to address this problem more effectively.

First Report—Assessing the Threat

The Advisory Panel produced a comprehensive assessment in its first report of the terrorist threat inside our borders, with a focus on chemical, biological, radiological, and nuclear (CBRN) weapons.

The very thorough analysis in that report can be summarized:

The Panel concludes that the Nation must be prepared for the entire spectrum of potential terrorist threats – both the unprecedented higher-consequence attack, as well as the historically more frequent, lesser-consequence terrorist attack, which the Panel believes is more likely in the near term. Conventional explosives, traditionally a favorite tool of the terrorist, will likely remain the terrorist weapon of choice in the near term as well. Whether smaller-scale CBRN or conventional, any such lower-consequence event—at least in terms of casualties or destruction—could, nevertheless, accomplish one or more terrorist objectives: exhausting response capabilities, instilling fear, undermining government credibility, or provoking an overreaction by the government. With that in mind, the Panel’s report urges a more balanced approach, so that not only higher-consequence scenarios will be considered, but that increasing attention must now also be paid to the historically more frequent, more probable, lesser-consequence attack, especially in terms of policy implications for budget priorities or the allocation of other resources, to optimize local response capabilities. A singular focus on preparing for an event potentially affecting thousands or tens of thousands may result in a smaller, but nevertheless lethal attack involving dozens failing to receive an appropriate response in the first critical minutes and hours.

While noting that the technology currently exists that would allow terrorists to produce one of several lethal CBRN weapons, the report also describes the current difficulties in acquiring or developing and in maintaining, handling, testing, transporting, and delivering a device that truly has the capability to cause “mass casualties.”

Second Report—Toward a National Strategy for Combating Terrorism

By the second year, the Advisory Panel shifted its emphasis to specific policy recommendations for the Executive and the Congress and a broad programmatic assessment and functional recommendations for consideration in developing an effective national strategy.

The capstone recommendation in the second report was the need for a comprehensive, coherent, functional national strategy: *The President should develop and present to the Congress a*

national strategy for combating terrorism within one year of assuming office. As part of that recommendation, the panel identified the essential characteristics for a national strategy:

- It must be truly *national* in scope, not just Federal.
- It must be comprehensive, encompassing the full spectrum of *deterrence, prevention, preparedness, and response* against domestic and international threats.
- For domestic programs, it must be *responsive to* requirements from and fully *coordinated with state and local officials* as partners throughout the development and implementation process.
- It should be *built on existing emergency response systems*.
- It must *include all key functional domains*—intelligence, law enforcement, fire services, emergency medical services, public health, medical care providers, emergency management, and the military.
- It must be *fully resourced* and based on *measurable performance*.

Of course, the Panel recognizes that in light of September 11, 2001 this objective has been difficult to achieve. However, the principles contained within this strategy and their requirements remain the same.

The Second Annual Report included a discussion of more effective Federal structures to address the national efforts to combat terrorism. We determined that the solutions offered by others who have studied the problem provided only partial answers. The Advisory Panel attempted to craft recommendations to address the full spectrum of issues. Therefore, we submitted the following recommendation: *The President should establish a senior level coordination entity in the Executive Office of the President.* The characteristics of the office identified in that recommendation included:

- Director appointed by the President, by and with the advice and consent of the Senate, at “cabinet-level” rank
- Located in the Executive Office of the President
- Authority to exercise certain program and budget controls over those agencies with responsibilities for combating terrorism
- Responsibility for intelligence coordination and analysis
- Tasking for strategy formulation and implementation
- Responsibility for reviewing State and local plans and to serve as an information clearinghouse
- An interdisciplinary Advisory Board to assist in strategy development
- Multidisciplinary staff (including Federal, State, and local expertise)
- No operational control

We included a thorough explanation of each characteristic in our Second Annual Report. For instance, we determined that this office should have the authority to direct the creation, modification, or cessation of programs within the Federal Interagency, and that it have authority to direct modifications to agency budgets and the application of resources. We also recommended that the new entity have authority to review State and geographical area strategic plans and, at the request of State entities, to review local plans or programs for combating terrorism for consistency with the national strategy.

Although not completely structured around our recommendations, the model for the creation of the Office of Homeland Security came from this recommendation.

To complement our recommendations for the federal executive structure, we also included the following recommendation for the Congress: *The Congress should establish a Special Committee for Combating Terrorism—either a joint committee between the Houses or separate committees in each House—to address authority and funding, and to provide congressional oversight, for Federal programs and authority for combating terrorism.* The philosophy behind this recommendation is much the same as it is for the creation of the office in the Executive Office of the President. There needs to be a focal point in the Congress for the Administration to present its strategy and supporting plans, programs, and budgets, as well as a legislative “clearinghouse” where relevant measures are considered. We recognize that Congress is still in the process of working towards this objective.

In conjunction with these structural recommendations, the Advisory Panel made a number of recommendations addressing functional requirements for the implementation of an effective strategy for combating terrorism. The recommendation listed below are discussed thoroughly in the Second Annual Report:

Enhance Intelligence/Threat Assessments/Information Sharing

- Improve human intelligence by the rescission of that portion of the 1995 guidelines, promulgated by the Director of Central Intelligence, which prohibits the engagement of certain foreign intelligence informants who may have previously been involved in human rights violations
- Improve Measurement and Signature Intelligence (MASINT) through an expansion in research, development, test, and evaluation (RDT&E) of reliable sensors and rapid readout capability and the subsequent fielding of a new generation of MASINT technology based on enhanced RDT&E efforts
- Review statutory and regulatory authorities in an effort to strengthen investigative and enforcement processes
- Improve forensics capabilities to identify and warn of terrorist use of unconventional weapons
- Expand information sharing and improve threat assessments

Foster Better Planning/Coordination/Operations

- Designate the senior emergency management entity in each State as the *focal point* for that State for coordination with the Federal government for preparedness for terrorism
- Improve collective planning among Federal, State, and local entities
- Enhance coordination of programs and activities
- Improve operational command and control of domestic responses
- The President should always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency

Enhance Training, Equipping, and Exercising

- Improve training through better coordination with State and local jurisdictions
- Make exercise programs more realistic and responsive

Improve Health and Medical Capabilities

- Establish a national advisory board composed of Federal, State, and local public health officials and representatives of public and private medical care providers as an adjunct to the new office, to ensure that such issues are an important part of the national strategy
- Improve health and medical education and training programs through actions that include licensing and certification requirements
- Establish standards and protocols for treatment facilities, laboratories, and reporting mechanisms
- Clarify authorities and procedures for health and medical response
- Medical entities, such as the Joint Commission on Accreditation of Healthcare Organizations, should conduct periodic assessments of medical facilities and capabilities

Promote Better Research and Development and Create National Standards

- That the new office, in coordination with the Office of Science and Technology Policy, develop a comprehensive plan for RDT&E, as a major component of the national strategy
- That the new office, in coordination with the National Institute for Standards and Technology (NIST) and the National Institute for Occupational Safety and Health (NIOSH) establish a national standards program for combating terrorism, focusing on equipment, training, and laboratory processes

Third Report—For Ray Downey

Our Third Annual Report to the President and the Congress builds on findings and recommendations in our First and Second Annual Reports delivered in 1999 and 2000. It reflects a national strategic perspective that encompasses the needs of all three levels of government and the private sector. It seeks to assist those who are dedicated to making our homeland more secure. Our recommendations fall into five categories:

- ✓ *Empowering State and Local Response* by ensuring the men and women on the front line of the war against terrorism inside our borders have the tools and resources needed to counter the murderous actions of terrorists;
- ✓ *Enhancing Health and Medical Capacities*, both public and private, to help ensure our collective ability to identify attacks quickly and correctly, and to treat the full scope of potential casualties from all forms of terrorist attacks;
- ✓ *Strengthening Immigration and Border Controls* to enhance our ability to restrict the movement into this country, by all modes of transportation, of potential terrorists and their weapons and to limit severely their ability to operate within our borders;
- ✓ *Improving Security Against Cyber Attacks* and enhancing related critical infrastructure protection to guard essential government, financial, energy, and other critical sector operations against attack; and
- ✓ *Clarifying the Roles and Missions for Use of the Military* for providing critical and appropriate emergency response and law enforcement related support to civilian authorities.

Mister Chairmen, I should note that the substance of all of the recommendations contained in the third report were approved by the panel at its regular meeting held on August 27 and 28, 2001—Tuesday the 28th being exactly two weeks prior to the attacks of September 11. Although we thoroughly reviewed those recommendations subsequently, the panel unanimously agreed that all were valid and required no supplementation prior to publication.

The recommendations contained in that report, listed below in summary form, are discussed in detail in the body of the report, and further supported by material in the report appendices, especially

the information from the nationwide survey of State and local responders covering an array of preparedness and response issues.

State and Local Response Capabilities

- Increase and accelerate the sharing of terrorism-related intelligence and threat assessments
- Design training and equipment programs for all-hazards preparedness
- Redesign Federal training and equipment grant programs to include sustainment components
- Increase funding to States and localities for combating terrorism
- Consolidate Federal grant program information and application procedures
- Design Federal preparedness programs to ensure first responder participation, especially volunteers
- Establish an information clearinghouse on Federal programs, assets, and agencies
- Configure Federal military response assets to support and reinforce existing structures and systems

Health and Medical Capabilities

- Implement the AMA Recommendations on Medical Preparedness for Terrorism
- Implement the JCAHO Revised Emergency Standards
- Fully resource the CDC Biological and Chemical Terrorism Strategic Plan
- Fully resource the CDC Laboratory Response Network for Bioterrorism
- Fully resource the CDC Secure and Rapid Communications Networks
- Develop standard medical response models for Federal, State, and local levels
- Reestablish a pre-hospital Emergency Medical Service Program Office
- Revise current EMT and PNST training and refresher curricula
- Increase Federal resources for exercises for State and local health and medical entities
- Establish a government-owned, contractor-operated national vaccine and therapeutics facility
- Review and recommend changes to plans for vaccine stockpiles and critical supplies
- Develop a comprehensive plan for research on terrorism-related health and medical issues
- Review MMRS and NDMS authorities, structures, and capabilities
- Develop an education plan on the legal and procedural issues for health and medical response to terrorism
- Develop on-going public education programs on terrorism causes and effects

Immigration and Border Control

- Create an intergovernmental border advisory group
- Fully integrate all affected entities into local or regional "port security committees"
- Ensure that all border agencies are partners in intelligence collection, analysis, and dissemination
- Create, provide resources for, and mandate participation in a "Border Security Awareness" database system
- Require shippers to submit cargo manifest information simultaneously with shipments transiting U.S. borders
- Establish "Trusted Shipper" programs
- Expand Coast Guard search authority to include U.S. owned—not just "flagged"—vessels
- Expand and consolidate research, development, and integration of sensor, detection, and warning systems
- Increase resources for the U.S. Coast Guard for homeland security missions

- Negotiate more comprehensive treaties and agreements for combating terrorism with Canada and Mexico

Cyber Security

- Include private and State and local representatives on the interagency critical infrastructure advisory panel
- Create a commission to assess and make recommendations on programs for cyber security
- Establish a government funded, not-for-profit entity for cyber detection, alert, and warning functions
- Convene a "summit" to address Federal statutory changes that would enhance cyber assurance
- Create a special "Cyber Court" patterned after the court established in FISA
- Develop and implement a comprehensive plan for cyber security research, development, test, and evaluation

Use of the Military

- Establish a homeland security under secretary position in the Department of Defense
- Establish a single unified command and control structure to execute all military support to civil authorities
- Develop detailed plans for the use of the military domestically across the spectrum of potential activities
- Expand training and exercises in relevant military units and with Federal, State, and local responders
- Direct new mission areas for the National Guard to provide support to civil authorities
- Publish a compendium of statutory authorities for using the military domestically to combat terrorism
- Improve the military full-time liaison elements in the ten Federal Emergency Management Agency region

Fourth Report—Implementing the National Strategy

Mr. Chairman and Members, as I mentioned earlier, the Advisory Panel release its fourth report to the President and the Congress on December 15, 2002. In addition to the comments in that report on the *National Strategy for Homeland Security* discussed earlier, the panel made 59 new policy recommendations in five key areas. I will summarize the rationale for each of those recommendations for the record

Organizing the National Effort

The new threat environment requires the consolidation in one entity of the fusion and analysis of foreign-collected and domestically-collected intelligence and information on international terrorists and terrorist organizations threatening attacks against the United States. *We recommend that the President direct the establishment of a National Counter Terrorism Center (NCTC).*

The FBI's long standing law enforcement tradition and organizational culture persuade us that, even with the best of intentions, the FBI cannot soon be transformed into an organization dedicated to detecting and preventing terrorist attacks. It is also important to separate the intelligence collection function from the law enforcement function to avoid the impression that the U.S. is establishing a kind of "secret police." *We recommend that the collection of intelligence and other information on international terrorist activities inside the United States, including the authorities, responsibilities and safeguards under the Foreign Intelligence Surveillance Act (FISA), which are currently in the FBI, be transferred to the NCTC.*

Focused and effective Congressional oversight of the domestic collection and analysis functions is required. Currently, the oversight of the FBI's FISA and other domestic intelligence activities is split between the Judiciary and Intelligence committees in each House of Congress. *We recommend that the Congress ensure that oversight of the NCTC be concentrated in the intelligence committee in each House.*

The *National Strategy for Homeland Security* designates various lead or co-lead agencies to perform both strategic and tactical analysis and vulnerability assessments. There is no indication that strategic assessments of threats inside the U.S. will receive dissemination to State and local agencies. *We recommend that the President direct that the NCTC produce continuing, comprehensive*

“strategic” assessments of threats inside the United States, to be provided to policymakers at all levels, to help ensure appropriate planning and allocation of preparedness and response resources.

It appears that the new DHS will have no authority for intelligence collection, limited capability for intelligence analysis, but significant responsibility for threat warnings. *We recommend that the Congress and the President ensure that the DHS has the authority to levy direct intelligence requirements on the Intelligence Community for the collection or additional analysis of intelligence of potential threats inside the United States to aid in the execution of its specific responsibilities in the area of critical infrastructure protection vulnerability assessments. We further recommend that the Congress and the President ensure that the DHS has robust capability for combining threat information generated by the Intelligence Community and the NCTC with vulnerability information the Department generates in cooperation with the private sector to provide comprehensive and continuing assessments on potential risks to U.S. critical infrastructure.*

The *National Strategy for Homeland Security* does not provide any clarity about the extent to which DHS will be “in charge” of executing a response during or after an attack on some CIP sector; nor does it specify which Federal agency is in charge for the Federal sector for other types of attacks. *We recommend that the President and the Congress clearly define the responsibilities of DHS and other Federal entities before, during, and after an attack has occurred, especially any authority for directing the activities of other Federal agencies.*

The question of who is in charge is especially problematic when it comes to a bioterrorism attack. No one in the Federal structure can currently identify who is or, even after DHS is formed, will be in charge in the event of a biological attack. *We recommend that the President specifically designate the DHS as the Lead Federal Agency for response to a bioterrorism attack, and specify its responsibilities and authority before, during, and after an attack; and designate the DHHS as the*

Principal Supporting Agency to DHS to provide technical support and provide the interface with State and local public health entities and related private sector organizations.

There are numerous Federal interagency coordination structures and several combined Federal/State/local structures. The proliferation of such mechanisms will likely cause unnecessary duplication of effort. *We recommend that the Assistant to the President for Homeland Security review and recommend to the President, and that the President direct, a restructuring of interagency mechanisms to ensure better coordination within the Federal government, and with States, localities, and the private sector, to avoid confusion and to reduce unnecessary expenditure of limited resources at all levels.*

The creation of DHS and the implementation of the *National Strategy* raise several legal and regulatory issues, not the least of which are quarantine, isolation, mandatory vaccinations, and other prescriptive measures. *We recommend that the President direct the Attorney General to conduct a thorough review of applicable laws and regulations and recommend legislative changes before the opening of the next Congress.*

The Congress is still not well organized to address issues involving homeland security in a cohesive way. Jurisdiction for various aspects of this issue continues to be scattered over dozens of committees and subcommittees. *We therefore restate our prior recommendation with a modification that each House of the Congress establish a separate authorizing committee and related appropriation subcommittee with jurisdiction over Federal programs and authority for Combating Terrorism/Homeland Security.*

Improving Health and Medical Capabilities

Officials in public health have indicated that it will take at least a five-year commitment from DHHS, at approximately \$1 billion per year, to have a material impact on States and local government

preparedness to respond to bioterrorist events. *We recommend that DHHS continue to provide financial support on the order of \$1 billion per year over the next five years to strengthen the public health system in the United States.*

The centralization and simplification of grants processes for public health and medical funds is essential to eliminate confusion and unnecessary redundancies. *We recommend that DHS coordinate and centralize the access to information regarding funding from various agencies such as DHHS (including CDC), EPA, USDA, and others and simplify the application process.*

There is currently no framework in place for monitoring the States' progress in meeting the objectives of the bioterrorism preparedness cooperative agreements program and for evaluating States' performance with respect to various outcomes. Moreover, there is a general lack of understanding on the part of representatives from State and local governments on precisely what they will be held accountable for and how their programs will be evaluated. *We recommend that DHHS, in consultation with State, local, and private sector stakeholders, establish and implement a formal process for evaluating the effectiveness of investment in State, local, and private preparedness for responses to terrorist attacks, especially bioterrorism.*

There are not yet widely agreed upon metrics by which to assess levels of preparedness among the medical and public health workforce. Without baseline data, it is impossible to quantify the gap between the current workforce and a workforce "prepared" to address these issues. *We recommend that DHHS fund studies aimed at modeling the size and scope of the healthcare and public health workforce needed to respond to a range of public health emergencies and day-to-day public health issues.*

Federal officials requested almost \$600 million to improve hospital preparedness for FY03. This level of funding is not sufficient to prepare the nation's 5,000 hospitals to handle mass casualty

events, mainly because hospitals, like public health agencies, have responded to fiscal pressures by cutting back on staff and other resources and otherwise reducing “excess capacity.” *We recommend that DHHS conduct a comprehensive assessment of the resources required by the nation’s hospital system to respond to terrorism, and recommend appropriate Federal-State-Local-Private funding strategies.*

The CDC needs to provide assistance in coordinating and connecting some of its own laboratory and disease surveillance information systems initiatives. These information systems should be connected to provide circular information flow. *We recommend that DHHS continue to strengthen the Health Alert Network and other secure and rapid communications systems, as well as public health information systems that generate surveillance, epidemiologic and laboratory information.*

Exercises are critical to ensure adequate training, to measure readiness, and to improve coordination. Resources directed to State and local entities to conduct these exercises have been limited and incentives for cross discipline coordination require strengthening. *We restate a previous recommendation with a follow on that the Congress increase Federal resources for appropriately designed exercises to be implemented by State, local, private sector medical, and public health and emergency medical response entities.*

There is an urgent need to clarify the role and functions of the various Federal and State emergency response teams and the extent to which their roles will be coordinated at the Federal, State, and local levels. *We recommend that DHHS clearly articulate the roles, missions, capabilities, and limitations of special response teams; that a plan be developed for the effective integration of such teams; and that focused training for special teams emphasize integration as well as coordination with States and localities.*

State and local officials require technical assistance from the Federal government to select among competing technologies, develop templates for communicating risks and information on actual events to the public, develop plans for surge capacity and pharmaceutical distribution, and provide adequate training to staff. *We recommend that DHHS evaluate current processes for providing required technical assistance to States and localities, and implement changes to make the system more responsive.*

Some State public health officials are unclear about their role in assisting with planning for the staffing of hospital beds in the state and otherwise becoming involved in surge capacity issues. States are implementing a wide range of preparedness activities but have had little opportunity to share this information with colleagues in other States. *We recommend that DHHS develop an electronic, continuously updated handbook on best practices in order to help States and localities more effectively manage surge capacity, the distribution of the National Pharmaceutical Stockpile, and other preparedness goals.*

In addition to the substantial research NIH is performing on prevention, treatment, and cures for bioterrorism agents, additional basic research and further research on the application of new technologies is urgently needed. *We recommend that NIH, in collaboration with CDC, strengthen programs focusing on both basic medical research and applied public health research, including the application of new technologies or devices in public health; and that DHS and OHS, in cooperation, prioritize and coordinate research among NIAID, other NIH entities, and other agencies conducting or sponsoring medical and health research, including DoD, DOE, and USDA, to avoid unnecessary duplication.*

The Model Health Powers Emergency Act would give State authorities certain important powers in a public health emergency. *We recommend that each State that has not done so either*

adopt the Model Health Powers Emergency Act, as modified to conform to any single State's special requirements, or develop legislation of its own that accomplishes the same fundamental purposes; and work to operationalize laws and regulations that apply to CBRN incidents—naturally occurring, accidental or intentional, especially those that may require isolation, quarantine, emergency vaccination of large segments of the population, or other significant emergency authorities.

During investigations into potential bioterror events, there is often a conflict between the goals and operating procedures of health and medical officials on the one hand and public safety officials on the other. The Federal Health Insurance Portability and Accountability Act (HIPAA) is in part designed to keep information about patients confidential and defines narrowly the information and the circumstances under which that information can be released. *We recommend that the Congress clarify the conditions under which public health agencies, EMS, and hospitals can share information with law enforcement officials in special emergency circumstances under HIPAA. We further recommend, as a prerequisite for receiving Federal law enforcement and health and medical funds from the Federal government, that States and localities be required to develop comprehensive plans for legally appropriate cooperation between law enforcement and public health, EMS and hospital officials.*

The development of a clear Federal strategic communications strategy, in coordination with State and local medical, public health, and elected officials, is not evident. *We recommend that DHHS, in coordination with DHS, develop an on-going, well coordinated strategy for education of the public on the prevention, risks, signs, symptoms, treatments, and other important health and medical information before, during and after an attack or large-scale naturally occurring outbreak occurs.*

There is still a lot to learn about the most effective ways to treat people with mental or emotional problems following a terrorist attack. *We recommend that DHHS, through the National Institute of Mental Health, and in collaboration with CDC, enhance funding for research into the prevention and treatment of the short and long-term psychological consequences of terrorist attacks.*

In-house health and medical expertise in the Intelligence Community is not sufficiently robust to provide for continuing strategic assessments of bioterrorism cause and effect. *We recommend that the Intelligence Community improve its capacity for health and medical analysis by obtaining additional expertise in the medical and health implications of various terrorist threats.*

A number of States came up short in their cooperative agreement proposals with respect to their plans for National Pharmaceutical Stockpile receipt and distribution. Federal technical assistance is needed by State and local health officials to develop and exercise these plans. *We recommend that DHHS significantly enhance technical assistance to States to help develop plans and procedures for distributing the NPS, continue to require exercises that demonstrate the States' ability to employ the NPS, and use specific metrics for evaluating States' capabilities.*

The timely research, development, production, and distribution of certain critical vaccines and other medical supplies continue to be perplexing problems. *We recommend that DHHS, in collaboration with DHS and DoD, establish a national strategy for vaccine development for bioterrorism that will be consistent with the nation's needs for other vaccines.*

Recently, Federal health officials recommended a multiphase smallpox vaccination program for at-risk emergency medical personnel, with the Federal government assuming liability for adverse events related to vaccination. *We recommend that the smallpox vaccination plan be implemented in incremental stages with careful analysis and continuous assessment of the risks of the vaccine. We further recommend that DHHS place a high priority on research for a safer smallpox vaccine.*

Defending Against Agricultural Terrorism

There is a lack of an overarching appreciation of the true threat to America's agriculture.

Without a broad threat assessment, it is difficult to prioritize resources to counter the terrorist threat.

We recommend that the President direct that the National Intelligence Council, in coordination with DHS, USDA and DHHS, perform a National Intelligence Estimate on the potential terrorist threat to agriculture and food.

The Animal Health Emergency Preparedness Plan provides a guide for comprehensive emergency management plans for the response to emergencies involving animals and the animal industry segment of production agriculture. The Emergency Support Function (ESF) in the Animal Health Emergency Preparedness Plan is not currently applicable to any ESF in the Federal Response Plan. *We recommend that the Assistant to the President for Homeland Security ensure that an Emergency Support Function for Agriculture and Food, consistent with the intent of the ESF described in the Animal Health Emergency Preparedness Plan, be included in the Federal Response Plan and the National Incident Response Plan under development.*

There are only two existing civilian bio-safety level 4 (BSL 4) laboratories for working with and diagnosing the most hazardous animal pathogens. If a large-scale outbreak of a foreign animal disease occurs in the United States, these would provide insufficient capacity. Capabilities at the State level would increase the ability to detect foreign animal diseases early. *We recommend that the President propose and that the Congress enact statutory provisions for the certification under rigid standards of additional laboratories to test for Foot and Mouth Disease and other highly dangerous animal pathogens.*

Without advance training, and the appropriate equipment and security in place prior to an outbreak, it is not likely that State veterinary labs will be adequately prepared to respond to a crisis.

We recommend that the Secretaries of Homeland Security and Agriculture (consistent with the November 2001 resolution of the United States Animal Health Association) jointly publish regulations implementing a program to train, equip, and support specially designated, equipped, secure, and geographically distributed veterinary diagnostic laboratories to perform tests and enhance surveillance for agricultural diseases that are foreign to the United States.

To encourage reporting of diseases and to ensure the stability of the agricultural sector, it is critical that a consistent scheme of national compensation is in place to provide financial assistance to producers and other agribusiness interests impacted by an animal disease outbreak. *We recommend that the Secretary of Agriculture, in consultation with State and local governments and the private sector, institute a standard system for fair compensation for agriculture and food losses following an agroterrorism attack; and that the Secretary of Health and Human Services should develop a parallel system for non-meat or poultry food.*

There are not enough appropriately trained veterinarians capable of recognizing and treating exotic livestock diseases in the United States. Other types of expertise required for dealing with agricultural diseases are lacking. *We recommend that the Secretary of Agriculture develop and that the Congress fund programs to improve higher education in veterinary medicine to include focused training on intentional attacks, and to provide additional incentives for professional tracks in that discipline. We further recommend that the Secretary of Agriculture, in coordination with States, improve education, training, and exercises between government and the agricultural private sector, for better understanding the agroterrorism threat, and for the identification and treatment of intentional introduction of animal diseases and other agricultural attacks.*

Improving the Protection of Our Critical Infrastructure

Physical and cyber infrastructure protection contains many very sensitive issues of great importance about which objective research and proposals are very difficult to conduct and develop within the political process. We have modified the recommendation in our *Third Report* to cover all infrastructures, both physical and cyber. *We recommend that the Congress establish and that the President support an Independent Commission to suggest strategies for the protection of the nation's critical infrastructures.*

The lack of a comprehensive assessment of threats to U.S. infrastructures significantly hampers defensive measures and preparedness activities. *We recommend that the President direct that the National Intelligence Council perform a comprehensive National Intelligence Estimate on the threats to the nation's critical infrastructure.*

The continuing bifurcation of policy for the physical and cyber components of CIP has created confusion and resulted in less than effective policy formulation. *We recommend that the President direct the merger of physical and cyber security policy development into a single policy entity in the White House.*

Progress in meeting airline passenger baggage-screening goals has been slow, and no screening technology will ever be foolproof. Perhaps equally important is the fact that much of the non-passenger cargo on commercial passenger aircraft is not being screened. *We recommend that DHS elevate the priority of measures necessary for baggage and cargo screening on commercial passenger aircraft, especially non-passenger cargo.*

The security of general aviation aircraft and facilities is thin, where it exists at all. *We recommend that that DHS, in conjunction with the airline industry, develop comprehensive guidelines for improving the security of general aviation.*

Hydroelectric and other dams on various watercourses present a significant hazard if terrorists find ways to exploit their controls. *We recommend that DHS make dam security a priority and consider establishing regulations for more effective security of dam facilities.*

One of the critical shortcomings in structuring programs and securing funds to protect critical infrastructures is the lack of risk-based models and metrics that help explain the value of protective measures in terms that public and private sector decision makers understand. *We recommend that DHS use the NISAC modeling and analytic capabilities to develop metrics for describing infrastructure security in meaningful terms, and to determine the adequacy of preparedness of various critical infrastructure components.*

*Establishing Appropriate Structures, Roles, and Missions for the
Department of Defense*

NORTHCOM is in a transitional phase between initial operational capability and full operational capability. In its initial structure, NORTHCOM has few permanently assigned forces, and most of them serve as part of its homeland security command structure. The creation of NORTHCOM is an important step toward enhanced civil-military integration for homeland security planning and operations, and could result in an enhancement of homeland security response capabilities. *We recommend that the Secretary of Defense clarify the NORTHCOM mission to ensure that the Command is developing plans across the full spectrum of potential activities to provide military support to civil authorities, including circumstances when other national assets are fully engaged or otherwise unable to respond, or when the mission requires additional or different military support. NORTHCOM should plan and train for such missions accordingly.*

In our *Third Report*, we recommended that a unified command be created “to execute all functions for providing military support or assistance to civil authorities”—an all-hazards approach. The Advisory Panel is pleased that NORTHCOM will apparently execute *most* of these functions, and

further *we recommend that the NORTHCOM combatant commander have, at a minimum, operational control of all Federal military forces engaged in missions within the command's area of responsibility for support to civil authorities.*

To achieve that clarity, the laws governing domestic use of the military should be consolidated and the Federal government should publish a document that clearly explains these laws. *We recommend that the President and the Congress amend existing statutes to ensure that sufficient authorities and safeguards exist for use of the military across the entire spectrum of potential terrorist attacks (including conventional, chemical, biological, radiological, and nuclear threats as well as cyber); that the authorities be consolidated in a single chapter of Title 10; and that DoD prepare a legal "handbook" to ensure that military and civilian authorities better understand the legal authorities governing the use of the military domestically in support of civilian authorities for all hazards—natural and manmade.*

No process is clearly in place to identify among the full scope of requirements for military support to civil authorities. *We recommend that the President direct the DHS to coordinate a comprehensive effort among DoD (including NORTHCOM) and Federal, State, and local authorities to identify the types and levels of Federal support, including military support, that may be required to assist civil authorities in homeland security efforts and to articulate those requirements in the National Incident Response Plan*

Insufficient attention has been devoted to planning and conducting military training specifically for the civil support mission. *We recommend that the Secretary of Defense direct that all military personnel and units under NORTHCOM, or designated for NORTHCOM use in any contingency, receive special training for domestic missions. Furthermore, in those cases where military*

personnel support civil law enforcement, special training programs should be established and executed.

There is a question about whether NORTHCOM's commander "combatant command" (COCOM) relationship with the various service component commands is only for the purpose of unity of *homeland defense* authority and responsibility or applies more broadly to all *homeland security* missions, including NORTHCOM's civil support mission. Thus, at this writing, the extent to which the new command will be able to direct new and expanded civil support training and exercises remains unclear. *We recommend that the Secretary of Defense clarify NORTHCOM's combatant command authority to ensure that Commander NORTHCOM can direct subordinate commands to conduct pre-incident planning, training, and exercising of forces required to conduct civil support missions.*

Rapid response-type capabilities should arguably be tailored to deal with homeland terrorist events that overwhelm State and local capabilities. *We recommend that the Combatant Commander, NORTHCOM, have dedicated, rapid-reaction units with a wide range of response capabilities such as an ability to support implementation of a quarantine, support crowd control activities, provide CBRNE detection and decontamination, provide emergency medical response, perform engineering, and provide communication support to and among the leadership of civil authorities in the event of a terrorist attack.*

States may have difficulty funding homeland security training and operations of the National Guard in State Active Duty status, especially if their missions are conducted for extended periods. Commanders are not clearly authorized under Title 32 to expend Federal funds for training for civil support tasks. *We recommend that the Congress expressly authorize the Secretary of Defense to provide funds to the governor of a State when such funds are requested for civil support planning, training, exercising and operations by National Guard personnel acting in Title 32 duty status and*

that the Secretary of Defense collaborate with State governors to develop agreed lists of National Guard civil support activities for which the Defense Department will provide funds.

The States' existing National Guard military support arrangements must be enhanced to provide for more effective response capabilities in Title 32 duty status. *We recommend that the President and governors of the several States establish a collaborative process for deploying National Guard forces in Title 32 duty status to support missions of national significance at the President's request; and that the Congress provide new authority under Title 32 to employ the National Guard (in non-Title 10 status) on a multi-State basis, and with governors' consent to conduct homeland security missions, and that the Secretary of Defense define clearly the appropriate command relationships between DoD and the National Guard. We further recommend that the Congress and DoD promote and support the development of a system for National Guard civil support activities that can deploy forces regionally--in coordination with DoD--to respond to incidents that overwhelm the resources of an individual State.*

Further enhancement of the National Guard's civil support capability and responsibility is necessary. In the *Third Report* we recommended "that the Secretary of Defense ... direct that National Guard units with priority homeland security missions plan, train, and exercise with State and local agencies," be expanded. *We now recommend that the Secretary of Defense direct that certain National Guard units be trained for and assigned homeland security missions as their exclusive missions (rather than primary missions as stated in our Third Report) and provide resources consistent with the designated priority of their homeland missions.*

Status of Our Recommendations

Mr. Chairman and Members, I can tell you that, according to our most recent count, of the 79 major policy recommendations made by the Advisory Panel in its first three reports, 64 have now been

adopted in whole or in major part. Having said that, there are others that continue to need to be addressed, and some that could still use additional resources or policy direction.

Conclusion

The Advisory Panel will continue to be relentless in pursuing appropriate solutions to these difficult issues, even if our recommendations are controversial and cross some “turf” boundaries. We will always—always—consider as an overarching concern the impact of any legal, policy, or process changes on our civil rights and liberties. Our Constitution, our laws, our judicial system, our culture, our history all combine to make our way of life unique in all the world.

Thank you again for this opportunity.

Mr. SHAYS. At this time we would call on Dr. O'Hanlon.

Dr. O'HANLON. Thank you, Congressman and Mr. Ranking Member. It is an honor to be before this committee on this important topic on this distinguished panel. I really want to just make three broad sets of opening comments in keeping with your request that we be brief. I have a longer statement, as you know, for the record.

Mr. SHAYS. I want to make sure, though, that you cover the territory that you need to.

Dr. O'HANLON. OK. Thank you. I do want to respond, and that is to your—to many of the questions that were posed to the first panel, and just give a couple of quick thoughts on the issue of how many strategies is too many and what kind of overall structure should we have. And I just have a couple of observations.

It strikes me that you do need more than one strategy, because there are so many aspects to the war on terror. And it is hard to put all this into one document, and I fully agree with Congressman Janklow's comment that if you have too many, you lose track of them all. But if you have too few, it would make, I think, for an excessively dense document that might get weighty of its own simple detail.

And so what I would propose is thinking in terms of three principle documents, and one is the National Security Strategy. And that has to be the lead document, has to be seen as the integrating document. Certainly in traditional terms that has been the first document that has been produced before the military has done its quadrennial reviews and its national military strategies. And then below that, the National Military Strategy and the National Homeland Security Strategy are the two natural next pillars.

And there are certain things that are going to be left out. Military strategy and homeland security strategy, for example, don't give a lot of time or attention to economic assistance toward developing countries. And we all know we need to worry about the problem of failed states, rescuing failed states, because they are a concern in the war or terror. They can be sanctuaries for terrorist organizations, they can help provide resources to terrorist organizations.

But that is part of the National Security Strategy, and I think President Bush—speaking of people who don't get enough credit, President Bush does not get enough credit for his foreign aid initiative, the millennium challenge account, which I think is a very good idea and I think needs more attention and more reinforcement, because we need to hold out hope to developing countries that they will be brought into this globalization procession, and that also we will prevent their territories from being used as sanctuary or sources of income for terrorists. So I commend the President on that point.

I think there is more that has to be done dealing with failed states, and I've got some of that in my testimony. But the National Security Strategy brings in economic assistance, brings in intelligence operations, brings in broader economic strategy as well. Those things are not part of the military strategy or the homeland security strategy quite as much, but that is OK. You don't have to emphasize each and every thing equally. At some point there is a tradeoff between having 12 or 15 or 20 strategies and having clar-

ity. And I think the National Security Strategy can provide enough detail on issues like economic policy toward developing countries and intelligence that we don't need major additional documents.

So again, that pyramid of three separate documents, National Security Strategy, Military Strategy, Homeland Security Strategy, for me is enough.

Mr. SHAYS. I feel like I'm in church.

Dr. O'HANLON. And I will stick with the trinity theme and go on now to my two other topics. One is on the issue of homeland security and the homeland security strategy, and now I am getting more specific.

Within this strategy I just want to make a couple of observations about how well this one particular strategy is working. It is so new, it is so important, and I think we have to spend a lot of time looking at it in detail. I will just offer a couple of thoughts based largely on the Brookings work that we have done in the last year and influenced by the work of the Gilmore Commission and others who preceded us with various studies.

And first of all, I want to commend the President and the Congress again for a very good start after September 11th. It seems to me there were a lot of very important things done immediately after the tragic terrorist attacks to make sure those sorts of attacks would be difficult to be carried out in the future against us; a lot of work on airport security, a lot of work on bringing together intelligence briefings for the President, a number of preparations on the biological weapons front largely motivated by the anthrax attacks. And I think a lot of that work was very good, but I think Congress and the President got bogged down a little in 2002. I think the debate over the Department of Homeland Security became seen as the big issue. And it was a big issue, but it can't be the only issue. We have to worry about our actual vulnerabilities, and we can't wait for Secretary Ridge to, 1 or 2 or 3 years from now, when he finally has his shop in order, get around to then addressing vulnerabilities. We have to have a debate today on the homeland security strategy and its specifics, what it does well, what it does not do well.

I think what it does well is to try to prevent the last kind of attack, try to prevent the last war, to use the old adage, about military operations. You know, people tend to fight the last or refight the last war. And I think we are getting pretty good at stopping airplane attacks, at stopping biological attacks. We haven't gotten as good at a number of other things, and let me just tick off a couple, and you are very well aware of them in this committee, but it is worth emphasizing.

For example, private sector infrastructure. There is this report that just came out that tries to be remedial and talk about some of the things we need to do, but it is not nearly enough. If you look around this country, there are thousands of chemical production facilities which are vulnerable to attack, and if they were attacked, they could produce clouds of toxic fumes that could produce threats to population centers similar to the Bhopal tragedy in India in the early 1980's. You could have thousands of people die from chemical fumes if these facilities were not well protected.

After September 11th, we did a very good job of trying to improve security at nuclear power plants, perhaps not enough, but we put quite a bit of effort into that, because there are only 103 of them, and we could focus on that problem. But meanwhile, you need to have a longer-term strategy for protecting chemical infrastructure. We have not really done that. So, the administration is trusting the private sector to protect its own assets, but an individual private sector owner or businessman, that person's incentives are different from society's because the individual owner is trying to make a profit, trying to deal with a competitor, and not very worried about a terrorist attack against his facility. The chances of that are astronomically low. So that person's incentives are to compete with his competitors; but as a society, our incentives are to make sure we're not vulnerable to catastrophic attack against our chemical facilities, against the trucking that ships a lot of these facilities, against a lot of the ships going into Houston and other ports that are carrying these sorts of chemicals.

Chemicals I just take as one example, but it is a very prominent example, and one that does not get the attention of nuclear issues, but probably should.

Another area within homeland security where we are not doing enough is the area of bolstering Customs. I think there was a great deal of good thinking done on Customs and the container security initiative last year by Mr. Bonner and others. A very good idea: Put American inspectors overseas and watch cargo being loaded before it heads toward American shores. The problem is we are not giving Mr. Bonner any resources to do this job more effectively. In the 2003 budget, there was no additional money, as I understand it, for this effort, and in the 2004 budget, Customs is supposed to get \$60—\$62 million more, not nearly enough for the kind of broader, more rigorous inspection regime we need.

We inspect 2 to 3 percent of all cargo entering this country. It is not nearly a high enough percentage. You don't need to reach 100 percent, but you have to do much better than we are doing today.

Another area within homeland security that is not getting enough attention is the surface-to-air missile threat against airplanes, and there has been a lot of discussion about this in the last few months since the attempted attack against the Israeli airliner. I think we need to consider government action to help airlines either protect themselves with countermeasures, or at a minimum help them and help airports patrol the grounds around the airport. This is a threat that has become very plain, and if those missiles had hit the airplane and brought it down, I am sure we would be responding much more quickly to what is a real threat around the world. And so we should not be taking great comfort in the fact those two missiles happened to miss by a small distance. They made the airplane feel a bump. How much more of a bump do we need? That's a pretty good impetus to policy right there, and yet we seem to be waiting for the airplane to actually be brought down before we make this a national priority.

One last area within homeland security, and then I will wrap up on my final topic. Information technology is a very important area to pursue and promote. As you know, Mr. Chairman, there is some

more money in the 2004 Homeland Security budget for information technology, but it really is not nearly enough, because today we are not able to integrate in a real-time basis State, Federal, local, international players into data bases that would look to try to connect dots. We can share information on suspicious individuals pretty fast, and that is a big improvement since September 11th. We can tell an airliner or somebody else, watch out for this individual, A, B, or C. That individual is on a terrorist watch list. That is a good improvement. However, we are not able to process information, the kind that we saw before the attacks in 2001, Phoenix memos, dots that need to be connected to discern patterns of terrorist behavior that may be emerging. We don't have the ability yet, in other words, to tie together these information systems in a large data base that's capable of processing and looking for patterns of behavior.

So we can share names, but that is not good enough. That is a very primitive level of information and infrastructure sharing of data. We have to do better.

Finally, on another matter, and I will just stop here after briefly mentioning the issue of preemption. And I know that time is out, so let me just quickly say, the preemption strategy is the national security strategy sort of benchmark or famous slogan that went along with the national security strategy last fall. To me, it shows that if you try too hard to make a splash with your national security strategy, you may get yourself into more trouble than you want. Sometimes it's better if these documents are a little more boring and understated, because I personally think the preemption concept is a major mistake as an articulated matter of national security policy. I think it's fine to find out——

Mr. SHAYS. Why don't we debate that issue with you. OK?

Dr. O'HANLON. OK. I will just quickly mention one last sentence, please.

For me, the problem is on North Korea. North Korea seems to have been influenced by this strategy. At least it's one possible explanation for the current crisis. And I worry that stating the doctrine so plainly has actually contributed to the crisis with North Korea. I like the logic behind the preemption concept, but I'm not sure the U.S. Government ought to be stating it so boldly and so plainly.

[The prepared statement of Dr. O'Hanlon follows:]

TESTIMONY ON NATIONAL COUNTERTERRORISM STRATEGIES BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND
INTERNATIONAL RELATIONS, HOUSE COMMITTEE ON GOVERNMENT REFORM

Michael O'Hanlon, mohanlon@brookings.edu, 202-797-6146, March 3, 2003

Thank you, Mr. Chairman and Mr. Ranking Member and other members of the committee, for the honor of being asked to testify on the critical subject of our nation's struggle against terrorism, and the administration's many strategies for countering this serious threat.

There are indeed a multitude of U.S. national strategies for countering terror. In fact, there probably are too many. It is hard to keep them straight, even for someone who tries to make it his business to follow them, and hard to know their relative importance and centrality in determining actual policy such as allocation of budget resources. There should be fewer.

For example, the national strategy for the physical protection of critical infrastructures and the national strategy to secure cyberspace could logically be part of the national strategy for homeland security. Also, one might merge the national strategy to combat weapons of mass destruction with the national military strategic plan for the war on terrorism.

But it is perfectly acceptable and reasonable to have several major strategy documents. Seven or eight seem too many, but three do make sense—a broad national security strategy, a national military strategy, and a homeland defense strategy. The specific purposes of each of these documents are different enough, and the key governmental players generally distinct enough, that some level of differentiation may be enriching rather than confusing.

That said, there are problems with each of the strategies on their own terms. My main points (some borrowed from coauthored work with Brookings colleagues) are as follows:

- On homeland security, the Bush administration’s basic strategy is a reasonable first effort, but fails to address several major national vulnerabilities, such as possible terrorist attacks against large private infrastructure, chemical facilities, and the trucking industry.
- Although the administration’s case for a greater emphasis on preemption has some merit, the decision to articulate it formally has caused us more harm than good. North Korea’s decision to accelerate its nuclear weapons program is probably exhibit A. (Other dimensions of the national security strategy are appealing, including the positive language towards China and the greater emphasis placed on foreign and economic assistance for developing countries.)
- Finally, in regard to military strategy, while many of Secretary Rumsfeld’s concepts are sound—revising the two-war framework, rethinking global basing, moving towards a limited national missile defense, encouraging joint-service experimentation, emphasizing “revolutionary” technologies and warfighting concepts—his plan has a major oversight in regard to the war on terror. Specifically, it does little to address the problem of failed states, where terrorists can take refuge or gain illicit resources that contribute to their strength and effectiveness. The U.S. armed forces cannot make nation building their primary task, but the United States does need to do more about quelling civil conflict and restoring stability to societies at war. For example, programs that help train and equip other countries’ militaries for conducting such missions need to be drastically expanded.

I now explore each of these issues in somewhat greater detail below.

HOMELAND SECURITY

This section draws on the preface to the second edition of our Brookings book, *Protecting the American Homeland*, that I coauthored with Peter Orszag, Ivo Daalder, Mac Destler, David Gunter, Jim Lindsay, Robert Litan, and James Steinberg.¹

¹ This book will be published by Brookings this spring.

Homeland security is daunting in its complexity, and in the sheer number of potential targets against which attack might be contemplated in an open country of nearly 300 million people. As such, it requires a conceptual foundation and set of priorities, if efforts are not to degenerate into a scattershot set of activities that leave many gaps and fail to make good use of available resources.

Recognizing as much, the Bush administration put forth a strategy for homeland security on July 16, 2002.² It was somewhat illogical that the strategy would be produced more than a month after the administration proposed a new department of homeland security, since the organization of the department should presumably be based on a clear sense of what it needs to accomplish. But as a practical matter, the strategy and the design of the department were designed largely in tandem, mitigating the downsides of this backwards approach.

The administration's strategy document recognizes that terrorists are themselves strategic, adaptive actors who will pursue new modes of attack and new weaponry. The administration's strategy makes particular reference to the further danger that terrorists will seek or obtain weapons of mass destruction. It emphasizes the necessary roles played by state and local governments as well as the private sector and individual citizens; indeed, according to administration estimates, the latter collectively outspend the federal government on homeland security efforts today (total national spending is about \$100 billion a year, of which the federal share is about \$35 billion).

The administration's strategy is similar in many ways to what Brookings proposed in April 2002. We suggested a four-tier approach to preventing terrorism in general, and catastrophic terrorism in particular: protect the country's borders, prevent attacks here at home by pursuing terrorists in the United States preemptively and keeping dangerous materials from them, protect key assets and population centers here at home as a final line of defense, and mitigate the results of any attacks that occur nonetheless. In short, our four-layered approach was border protection, domestic prevention, domestic protection, and consequence management.

² See Office of Homeland Security, *National Strategy for Homeland Security* (July 2002), available at www.whitehouse.gov.

The Bush administration proposes a six-tier approach, involving six “critical mission areas.” The first is intelligence and warning, followed by border and transportation security, domestic counterterrorism, protecting critical infrastructures and key assets, defending against catastrophic threats, and emergency preparedness and response. The administration also proposed four key methods or “foundations” for enhancing all six tiers of defense: law, science and technology, information sharing and systems, and international cooperation. One can always quibble with specifics; for example, the Bush administration’s critical mission area of intelligence and warning seems more of a foundation or method than a separate tier of defense. But the taxonomy serves its main purposes well.

Although the administration’s strategy makes a start, it leaves out several key priorities for action. They can be organized into three broad categories. One concerns major infrastructure in the private sector, which the Bush administration largely ignores. A second concerns information technology and its proper uses; despite rhetoric about using IT aggressively to promote homeland security, the Bush administration budgets and programmatic activities to date do not match the rhetoric. A third concerns the presently unrecognized need to greatly expand certain specific capacities for homeland security such as the Coast Guard and Customs.

Regarding the private sector, the Bush administration is too willing to take a free-market approach, trusting owners of large buildings, factories, and other facilities to deduce what protection they need and provide it largely on their own. But the business of American business is business, not homeland security. It is therefore not surprising that, for example, the chemical and trucking industries have not moved adequately on their own to improve safety, leaving their assets vulnerable to theft or sabotage.

In regard to information technology, the administration still has no plan for quickly improving real-time information sharing not only in the national law enforcement community, but among the broader set of public and private actors who are vital to preventing and responding to homeland attacks. And its investments to improve information sharing throughout the government fall woefully short of what is needed. Investments of more than \$10 billion will be

needed if government at all levels is to be capable of “connecting the dots” the next time around. We can share databases on terrorist suspects quickly today, a considerable accomplishment since 9/11, but that is not enough.

Finally, while the administration plans to modernize the Coast Guard and adopt a new approach to Customs, it does not recognize the need to increase the overall size and capacity of these organizations. The former was already undersized for a wide variety of missions it performed before 9/11, when homeland security imperatives then demanded more than half its fleet (and continue to employ perhaps a quarter of it). The latter still only inspects less than 5 percent of all cargo entering the country, even if it has become savvier about small percentage to examine. The container security initiative, and placing U.S. inspectors in many overseas ports where cargo can be monitored before reaching the United States, is a very good idea, but it is underfunded by an order of magnitude in the 2004 budget proposal. Indeed, all of the shortcomings of the administration’s homeland security plan are reflected in not only the homeland security strategy document, but the administration’s budget proposal for 2004 and its critical infrastructure and cyberspace strategies as well.

THE NATIONAL SECURITY STRATEGY AND PREEMPTION

The new shift in emphasis on preemptive and preventive uses of force is a response to the terrorist attacks of Sept. 11, 2001, which brought home the necessity to address potentially catastrophic threats before the country can be attacked. The first manifestation of this more forceful attitude was the president’s seminal Sept. 20, 2001, speech to a joint session of Congress vowing to hold responsible the terrorists as well as those who harbor them. It paved the way for a largely successful military campaign in Afghanistan and sent a clear warning to other state sponsors of terrorism.³

³ This section focuses on the Bush administration’s so-called doctrine of preemption and is drawn largely from a Brookings policy brief coauthored late last year with James Steinberg and Susan Rice.

The preemption concept was further elaborated in the president's West Point speech and then more formally in the National Security Strategy. It threatens to attack so-called rogue states, which pose a danger to the United States, whether or not they are demonstrably linked to terrorist organizations of global reach. The administration argues that the continued spread of weapons of mass destruction (WMD) technology to states with a history of aggression creates an unacceptable level of risk, and presents "a compelling case for taking anticipatory actions to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack."

However, a broad-based doctrine of preemption carries serious risks. The Bush administration was right to take a strong stand against terrorists and extremist states, but it had already accomplished this goal with its early words in the period after the September 11 attacks and its actions in Afghanistan. It did not need a formal doctrine of preemption to drive the point home. Rather than enunciate a formal new doctrine, it would have been better to continue to reserve the preemptive military tool for a narrow, rare class of situations where inaction poses a credible risk of large scale, irreversible harm and where other policy tools offer a poor prospect of success. Given that the doctrine has now been promulgated, the Bush administration should clarify and limit the conditions under which it might be applied.

Elevating the preemptive option to a policy doctrine can have serious negative consequences. For one, it reinforces the image of the United States as too quick to use military force and to do so outside the bounds of international law and legitimacy. This can make it more difficult for the United States to gain international support for its use of force, and over the long term, may lead others to resist U.S. foreign policy goals more broadly, including efforts to fight terrorism. Elevating preemption to the level of a formal doctrine may also increase the administration's inclination to reach for the military lever quickly, when other tools still have a good chance of working.

Advocating preemption warns potential enemies to hide the very assets we might wish to take preemptive action against, or to otherwise prepare responses and defenses. In this tactical sense, talking too openly about preemption reduces its likely utility, if and when it is employed.

Finally, advocating preemption may well embolden other countries that would like to justify attacks on their enemies as preemptive in nature.

One can argue that a more explicit policy of preemption actually reinforces deterrence by putting other countries on notice about America's seriousness of purpose in addressing threats such as the possession of weapons of mass destruction by rogue regimes. It also allows the administration to argue that its focus on Iraq is part of a broader security concept and does not represent preoccupation with a specific regime. However, linking the real problem of Iraq's weapons of mass destruction (WMD) to a broader doctrine of preemption (defined to include preventive war) complicated the administration's task in gaining international support for its preferred policy last fall, and may be contributing to our diplomatic difficulties at present as well. Bizarrely, many countries seem to worry as much about restraining the United States as about disarming Saddam—not a defensible position on their part, but a reality nonetheless, and one that the preemption doctrine may have helped create.

Many countries worry that the Bush administration will take a similar preemptive and largely unilateral approach in dealing with other cases such as North Korea or Iran or Syria. Further, other countries' frustration with the United States' decision to grant to itself, (though not to others), a right of preemption may chill their willingness to cooperate fully with the United States in the war on terrorism. To date, that does not seem to be a major problem, but the situation could change.

THE NATIONAL MILITARY STRATEGY AND FAILED STATES

Finally, the administration's strategies for dealing with terror do not have a strong plan for helping failed states—the current or future Afghanistans where al Qaeda could find refuge and resources.

There are many tools needed to reduce the prevalence of failed states. But some have to do with the physical capacity to forcibly stop or mitigate conflict in some situations, and to help keep the peace after parties to a war have agreed to a ceasefire on their own in others.

Today, unfortunately, most countries besides the United States do not have the wherewithal to deploy well-equipped troops quickly and effectively to trouble spots, and then to keep them there once they have been deployed. Surveying the world's conflicts, both those now underway and those of the recent past, it would be desirable that the international community have roughly double its current capacity to deploy and sustain forces abroad. It has been averaging about 100,000 forces in various peace and stabilization missions in recent years, but a survey of the world's hotspots suggest that it would often be useful to be able to deploy and sustain 200,000 troops for such missions.⁴ As noted, these missions are important not only for humanitarian reasons, but for national security ones as well—to deprive terrorists of sanctuaries and sources of income (from diamonds, drug trading, and the like) that they can often obtain in failed or failing states.

Since some countries will choose not to participate in any given operation, and since troops will need to be rotated to avoid exhaustion and burnout, a total pool of perhaps 600,000 personnel would be desirable. That number is not exact; it is hard to know how troop rotations would work in advance. But a three-to-one ratio of available forces to deployed forces has generally been considered appropriate by the U.S. military. If anything, it is optimistic, and even more than 600,000 could be required to maintain 200,000 on deployment.⁵ The international community already has about that number of military personnel who can be rapidly deployed and then sustained in overseas theaters. The problem, however, is that two-thirds of the total number now comes from the United States. But there is no reason the United States should be expected

⁴ See my recent book, *Expanding Global Military Capacity for Humanitarian Intervention* (Brookings, 2003).

⁵ In fact, on average the United States maintains no more than 10 percent of its forces on deployment, away from home station, at a time—somewhat more than 100,000 out of a total active-duty personnel strength of 1.4 million. Indeed, it considers that level of effort rather onerous. But that aggregate figure of 1.4 million includes many non-combat troops, so the ratio may be misleading. As another means of estimating availability, note that most U.S. military services have a policy of not having individual personnel be absent from home for more than 120 days a year, essentially revalidating the 3:1 rule. See Michael O'Hanlon, *Defense Policy Choices for the Bush Administration* (Washington, D.C.: Brookings, 2001), pp. 22-58.

to provide most forces for such missions, and as a practical matter, this country will not be willing or able to do so in any event.

For these reasons, if there is to be additional effort in humanitarian and peace operations in the future, most is likely to come from other countries. That means that of the desired pool of 600,000 deployable military personnel, non-U.S. countries should provide about 500,000 of the troops. In other words, countries besides the United States should more than double their aggregate power projection capabilities.

That number should be sobering for those who consider humanitarian military operations to require only relatively modest amounts of force. But it should be within reach for the international community, if not right away, then over time. To begin, not all troops need be equally well trained and equipped. Some missions will be less demanding than others. Some will not require rapid response or long-range transport. Either the peace accords that precede them will be negotiated over an extended period, allowing ample time for preparations, or the operations will be close to home for countries contributing troops. Even if 200,000 forces might be needed at a time, it is unlikely that it would be necessary to deploy more than 50,000 urgently, and unlikely that more than half to two-thirds would need to operate in extremely austere surroundings.

Although their situations vary greatly from region to region and country to country, developing countries face many common budgetary challenges in any effort to expand military capabilities. The costs would follow from the need for more rigorous training and for better equipment.

Particularly in Africa, a continent facing many acute economic problems, the western powers will need to provide many of the resources required to expand and improve regional military capabilities. Programs now underway, such as the U.S. Africa Crisis Response Initiative (recently renamed the African Contingency Operations and Training Assistance program, or

ACOTA), are important steps in the right direction. But they do not involve nearly enough troops or provide sufficiently rigorous training and sufficiently capable equipment.

The need for more rigorous training is evident. Under current assistance programs, exercises and classes typically take no more than a few weeks. Yet creating a highly ready military, competent across a broad spectrum of operations including combat, typically takes many months if not longer.⁶ As a U.S. Army field manual puts it, “The most important training for peace operations remains training for essential combat and basic soldier skills”—underscoring the scope of the challenge for preparing good troops for such missions.⁷ In addition, troops conducting peace and humanitarian interventions also must work with nongovernmental organizations that provide relief and other services, adding further complexities to any mission.⁸ The United States and other foreign militaries cannot be expected to build other countries’ armed forces up from the ground level; nor would any such offers necessarily be well received. But months of training, as opposed to weeks, are needed. So are refresher courses every one to two years. At least a doubling in the intensity of training per unit is appropriate. Exercises are also needed to practice coordinating operations at higher and larger levels of effort—notably, for missions involving brigades and divisions. Most of these exercises can be headquarters and staff efforts, as opposed to full-scale field training, but they are critical.

To get a handle on the costs of serviceable equipment for such countries, two different approaches can be taken. One is to examine the costs of a country such as Turkey or South Korea—a country that has typically tried, and succeeded, to field strong ground forces with fairly low defense spending. This approach tends to produce cost estimates that are somewhat too low, perhaps, since such countries do not typically buy large amounts of strategic lift or deployable logistics support equipment.

⁶ For a good explanation of how hard the U.S. military needed to work to improve its own standards after Vietnam, see Robert H. Scales, Jr., *Certain Victory: The U.S. Army in the Gulf War* (Washington, D.C.: Brassey’s, 1994), pp. 1-38.

⁷ U.S. Army, *Field Manual 100-23: Peace Operations* (Washington, D.C., 1994), available at www.adtdl.army.mil/cgi-bin/atdl.dll/fm/100-23/fm100-23.htm, chapter 3, p. 8.

⁸ See for example, Chris Seiple, *The U.S. Military/NGO Relationship in Humanitarian Interventions* (Carlisle Barracks, Pa.: U.S. Army War College Peacekeeping Institute, 1996); Byman et.al., *Strengthening the Partnership*.

Another way is to examine the U.S. Marine Corps budget. Since the Marines are very sustainable abroad, their budget does cover the costs of deployable logistics (though not the costs of strategic transport, which are provided for them by the Air Force and especially the Navy). Cost estimates produced in that way may wind up high, however, given the more costly equipment usually purchased even by the most frugal of the U.S. military services. But it explicitly accounts for support forces of various types—medical crews, engineering and construction companies, firefighting units, communications specialists, and so forth—that are just as critical in many operations as infantry soldiers themselves. An international effort to improve African capacities should aspire to attain levels as close to those of the Marine Corps as possible, given the desirability of possessing organic logistics support capabilities and combat capabilities in regions far removed from the domestic infrastructure of the country in which a conflict occurs. But useful benefits can be attained at lower levels of effort as well.

South Korea has, over the past couple of decades, averaged spending some \$10 billion to \$12 billion on its military, with about \$3 billion to \$4 billion typically going to procurement.⁹ With that budget, it fields half a million active-duty ground forces, most of them light infantry but with substantial numbers of armored and mechanized formations as well. In other words, the types of units in South Korea's military are probably a good model for what one would want to create in the way of global intervention capacity. Since South Korea's equipment inventories have been built up over two to three decades, given the normal lifetimes of most weaponry, and since a good deal of its procurement budget has gone to its air force and navy, its ground forces probably field about \$50 billion in equipment. Since they number 450,000 troops, the value of their equipment is roughly \$10 billion per 100,000 soldiers.

As for the U.S. Marine Corps, over the past 20 years it has typically spent \$1.5 billion to \$2 billion procuring ground-combat equipment for nearly 200,000 Marines. So it has acquired

⁹ See various issues of the International Institute for Strategic Studies' *Military Balance* (current issues are published by Oxford University Press), as well as Ministry of Defense, *Defense White Paper 1997-1998* (Seoul, 1998), pp. 136, 190.

\$30 billion to \$35 billion in equipment for 150,000 Marines focused on ground combat. These numbers suggest a cost of about \$20 billion per 100,000 ground troops.

Suppose that the world's developing countries chose to develop well-equipped deployable ground forces including 100,000 soldiers, as well as comparable numbers of well-trained soldiers with somewhat less equipment and more limited capabilities. The cost for the first 100,000 soldiers might then be \$10 billion to \$20 billion, and the cost of the second group perhaps half as much. (If the purchases were not done in a coordinated manner, unit costs might go up somewhat, as would subsequent maintenance costs. On the other hand, if second-hand equipment were sometimes acquired, costs could be less.)

Poor countries, principally in Africa, might receive such equipment as aid. The donor community might spend up to \$20 billion to make such an arrangement work. The U.S. share might be \$7 billion to \$8 billion, assuming that Europe would provide an equal amount and that countries such as Japan would contribute significant assistance as well. If provided during a ten-year initiative, annual U.S. aid would be about \$750 million for this purpose; operating and training costs could drive the total close to \$1 billion. Including support from all donors, annual costs would total \$2 billion to \$3 billion a year.

The proposed U.S. assistance figure is dozens of times higher than past spending for the Africa Crisis Response Initiative plus Operation Focus Relief combined, and comparable to the entire U.S. assistance budget for Africa. But it is several times less than current U.S. military aid to the Middle East. Total assistance under this proposal from all donors would be several times less than what Africans themselves spend on their armed forces (about \$10 billion a year) and almost ten times less than total economic aid to Africa (about \$20 billion a year). Moreover, such levels need not be attained overnight, if at all, for an effort of some substantial type to be desirable. This calculation is an estimate of what it would cost to create an idealized intervention and peacekeeping capability for the international community. Much more modest, and politically realistic, efforts would themselves be highly useful.

Substantial numbers of U.S. personnel might be needed to carry out the associated training. For example, 150 special forces personnel were involved in Operation Focus Relief in 2001, for a program training just 4,000 troops.¹⁰ Were that program increased by a factor of ten, more than 1,000 special forces troops might be needed, out of a total of only 30,000 active-duty special forces in the U.S. inventory. However, such a large number of special forces could not realistically be provided, so private contractors such as MPRI would probably have to be hired, adding several tens of millions of dollars to the required annual budget. Such an additional expense is well worth it given the severity of the problem of civil violence in the world today.

CONCLUSION

Mr. Chairman and Mr. Ranking Member, the Bush administration has made important progress on a number of fronts in the struggle against terrorism. But there are holes in its homeland security strategy and its national military strategy, including poor protection for the chemical industry and for skyscrapers in the first case, and insufficient attention to the problem of failed states in the second. There are also unfortunate aspects, notably the doctrine of preemption, to its national security strategy. The Congress needs to provide oversight and pressure to help the administration with its task. Unfortunately, the proliferation of counterterrorism strategy documents makes the job somewhat harder. But if one thinks in terms of three broad areas of effort—homeland security, military strategy, and broader foreign policy/security policy—the conceptual challenge becomes more manageable. I thank you for the opportunity to testify today.

¹⁰ Segun Adeyemi, "Special Forces Teach Peace Support Skills," *Jane's Defence Weekly*, May 23, 2001.

Mr. SHAYS. I was trying to figure out why I liked you, and then reviewed your bio, and you were a former Peace Corps volunteer, and so that speaks well of you, sir.

Dr. O'HANLON. Thank you.

Mr. SHAYS. Mr. Newhouse.

Mr. NEWHOUSE. Thank you, Mr. Chairman. I appreciate the opportunity.

Mr. SHAYS. If you could turn on your mic. Is it turning on? The green light should do it. If it's orange, watch out.

Mr. NEWHOUSE. I was about to say, I appreciate the opportunity to offer a few thoughts with regard to this tough and complex subject you are dealing with.

Mr. SHAYS. Well, we appreciate you being here, sir.

Mr. NEWHOUSE. And I would like to make a few comments on our government's approach to various sources of instability as I see them since the attack of September 11th.

Huge opportunities were left in the wake of September 11th. Stated simply, most of the world was ready and willing to accept American leadership. We are all Americans, proclaimed the page 1 head line in Le Monde, on September 12th, a declaration of solidarity from a most improbable source.

In seizing the moment, the administration could and should have set about stabilizing the most serious sources of instability, the Middle East, Southwest Asia, and Northeast Asia. In the Middle East, they could have deployed their new leverage to push Israel and the Palestine Liberation Organization into serious negotiations. Quite clearly, Israel's Likkud Government expected exactly that to happen, especially when on October 2nd, Mr. Bush endorsed the idea of a Palestinian State. Two days later, Prime Minister Ariel Sharon warned Washington not to try to appease the Arabs at our expense. Israel will not be Czechoslovakia, he said. The administration listened. Regime change on the West Bank became more attractive than taking on Israel's Likkud Government and its allies in Washington.

Since World War II, the Arab world has been largely shaped by transient passions, notably anticolonialism, nationalism, socialism, and Islamism. The single constant, apart from corrupt and/or incompetent regimes has been the Arab-Israeli conflict, and a perception throughout the region and most of the world that Washington shares responsibility with Israel for the plight of the Palestinian people.

In his speech last week, Mr. Bush offered some hope saying that, "If the terror threat is removed and security improves," Israel, "will be expected to support the creation of a viable Palestinian State. As progress toward peace develops, settlement activity in the occupied territories must end."

Mr. SHAYS. Excuse me, Mr. Newhouse, I'm going to have you move the mic down a spec. Just bring it down a little bit. It's on.

Mr. NEWHOUSE. However, Mr. Bush provided no specifics. Who will judge whether the terror threat has been removed or sufficient progress toward peace has been made? A skeptic would say that if the recent past is any guide, Israel's Prime Minister Mr. Sharon will make those calls.

On April 4 last year, Mr. Bush said, "Enough is enough." And he added, "I ask Israel to halt its incursions into Palestinian-controlled areas and to begin the withdrawal from those cities it has recently occupied. Israeli settlement activity in occupied territories must stop, and the occupation must end through withdrawal to secure and recognizable boundaries."

Mr. Bush also announced that he was sending Secretary Powell to the Middle East to push for a political settlement. Two days later Mr. Bush called Sharon and said: Israel must pull its forces out of the West Bank, "without delay." And the White House appeared to support Secretary Powell's idea of bringing the parties together in a peace conference. Then Mr. Powell left on a 6-day trip to the region, and General Anthony Zinni, the President's special envoy for the Middle East, conveyed to Sharon Mr. Bush's call for Israel to withdraw at once from Palestinian cities.

On April 9th, 3 days after the call from the President, Mr. Sharon said that Israel would press on with its offensive in the West Bank.

On April 17th, Powell returned without the cease-fire he had been seeking and unable to secure a withdrawal of Israeli forces from the West Bank. Meanwhile, Ari Fleischer, the White House press spokesman, was stressing that Sharon was, "a man of peace."

The tilt toward Mr. Sharon reached a peak of sorts on June 24, 2002, when Mr. Bush told the Palestinian people they would have to replace Yasser Arafat as their leader before Washington would support an independent Palestinian State. Without mentioning Arafat by name, the President made his meaning clear, "Peace requires a new and different Palestinian leadership so that a Palestinian State can be born." Until then, Mr. Bush has resisted the Sharon position that no negotiations could take place until Arafat was gone. Polls on the West Bank have shown that Arafat's approval rating has steadily declined in recent years; it spikes, however, when he is attacked by Sharon. They appear to need each other.

Again, in last week's speech, Mr. Bush made the case that regime change in Iraq would provide the conditions for weakening terrorism and helping Palestinians achieve democracy. I disagree. The case for and against attacking Iraq now is complex. It should not be tied into the campaign against terrorism. The connection between Iraq and terrorism is, I think, tenuous at best. Most of the people I know who have followed the affairs of the Middle East over the years would argue that the single unchanging precondition for regional peace and stability is measured but steady progress toward a settlement of the Palestinian issue, starting with an end to Israel's occupation of the West Bank.

If the United States gets too far adrift from reality in the Middle East, the sole beneficiary would be Usama bin Laden and his legatees if he is dead. Their purpose, indeed their *raison d'etre*, is to divide the West from Islam, starting with the Arab world.

In the Persian Gulf, the Iranian Government reacted to September 11th by authorizing American search and rescue operations on its soil, the transit of humanitarian assistance and cooperation in the formation of the new Afghan Government. In many Iranian cities there were meetings to express sympathy for the victims of the

attacks on the United States. Both hard-liners and reformers denounced the attacks, and at that pivotal moment, Iran's reformist government would probably have been politically free to extend its reach to America even further. The combination of sensible steps by Washington on the Arab-Israeli front and improved U.S.-Iranian relations would have further isolated Iraq politically within the region and, hence, appealed to all sides. But the administration's failure to respond and its harsh reaction, notably the President's axis of evil remark, damaged prospects for beginning to repair a bilateral relationship with Iran of surpassing strategic importance.

Pakistan, a nominal ally, is the country that most nearly fits the President's profile of evil. Two of its provinces are controlled by Taliban and al Qaeda sympathizers. Although the issues that divide Iran and Pakistan have never reached the level of crisis, relations have worsened in recent years. Pakistan's heavy involvement with the Taliban is partly responsible. It is a bone—the Taliban is a bone in Iran's throat. Pakistan's Islamic schools, the madrassas, have become training grounds for terrorists and other radical groups in much of the Muslim world.

For now there may be little that the Musharraf government can do about the chaos and anarchy in parts of the country, but it can and should be held to account for its remarkable decision to make possible North Korea's highly enriched uranium program. Pakistan is known to have provided much or most of the program, weapons design, gas centrifuges, materials to make centrifuges, data of the sort that would enable the customer to avoid having to test its devices. The two-way traffic between Pakistan and North Korea involving ballistic missiles and nuclear weapons technology could have a dangerous ripple effect.

The campaign against terrorism generated a sense of common purpose, but at another level also became divisive. Most of Mr. Bush's advisors regard the first and best answer to threats to security as lying in preponderant military force. European governments along with most others see military force as a complementary tool in the campaign against terrorism, less essential than a soft-power mix of intelligence, law enforcement, border, and financial controls.

Terrorism is generally seen as part of a larger problem, not a single problem. Thus far, however, the administration's concern with the causes of terrorism has been minimal, in my view. Its focus instead has been on identifying and destroying the terrorist threat, "before it reaches our borders," if necessary, acting alone and using preemptive force. This thinking is contained in the novel doctrine laid down by the administration last September.

Other governments assume, doubtless correctly, that in its reliance on massive military power, the new doctrine downgrades alliances. They also worry that the administration may not feel bound by the body of international rules and restraints that developed after World War II. Taken at face value, the new doctrine justifies preventive war waged without allies and without U.N. Sanction.

A doctrine of preemption that relied on very high-quality intelligence to identify an impending attack well in advance and then head it off would not raise eyebrows, but the Bush doctrine is based instead on prevention and preeminence; that is, taking military power to a level never before seen, one that would so intimi-

date all parties that no one would even consider an attack of any kind against the United States. Threats to American interests would be not just discouraged, but precluded. "Full spectrum dominance," was a term for it in defense circles. Anticipatory self-defense is a phrase that Secretary Rumsfeld has used.

In practice, such a doctrine harbors many risks. If I am banging on too long, please cut me off, Mr. Chairman.

Mr. SHAYS. Keep going.

Mr. NEWHOUSE. It exaggerates the role and utility of raw military power. The government could find itself unable to carry out programs in other realms, unable, for example, to cooperate effectively with other governments to combat terrorism. Special Forces and smart weapons can help in that battle, but other tools starting with good intelligence and good police work are more important.

No matter how good the performance of the Intelligence Community, surprises are probably unavoidable. Thus, measuring performance by the standard of prediction is unrealistic and can damage the standing, morale, and performance of intelligence agencies. They are engaged in not winning a war against terrorism, but in managing it, restricting the activities and options of hostile forces. The Bush doctrine, if taken seriously, would mean that prediction would become the measure of performance, because a prevention-based strategy would require sustained and timely collection of the kind of intelligence that is rarely available, least of all in a form that connects all the dots.

Effective intelligence collection must be conducted bilaterally, but with a wide array of countries. After September 11th, offers of help, large and small, poured into Washington from around the world. They were rejected. Another opportunity lost. Accepting these offers would have harmed nothing, generated enormous goodwill, and, most important, helped at another more important level. What the United States has needed from other countries, then as now, is information, a process through which intelligence may be shared with countries best equipped to penetrate terrorist organizations and cells. Many of these countries took part in the sanctions against Iraq, and most of them have experienced serious difficulties of one kind or another with the terrorist groups located in the extensive region they share.

Terrorism may be contained if intelligence services and police agencies acquire the habit of cooperating closely with each other and suppressing their competitive instincts and preference for acting alone. The United States would be the chief beneficiary of such activity, first because it appears to be the primary target of al Qaeda and sibling terrorist groups; second, because it lacks adequate human resources for gathering the intelligence it needs; and third, because its ability to eavesdrop on global communications is declining. The rapid growth of commercially available technology is reported as allowing for the creation of all but unbreakable computer codes. Fiber-optic lines give off no electronic signals that can be monitored.

Mr. Chairman, that concludes my statement. Thank you.

Mr. SHAYS. Thank you.

[The prepared statement of Mr. Newhouse follows:]

119

Statement of John Newhouse

Senior Fellow

Center for Defense Information

House Committee on Government Reform,

**Subcommittee on National Security, Emerging Threats and
International Affairs**

March 3, 2003

Huge opportunities were left in the grim wake of September 11. Stated simply, most of the world was ready and willing to accept American leadership “We are all Americans,” proclaimed the page one headline in *Le Monde* on Sept. 12, a declaration of solidarity from an unlikely source.

In seizing the moment, the administration could and should have set about stabilizing the most serious sources of instability—the Middle East, Southwest Asia and Northeast Asia. In the Middle East, they could have deployed their new leverage to push Israel and the Palestine Liberation Organization (PLO) into serious negotiations. Quite clearly, Israel’s Likud government expected exactly that, especially when on October 2, Mr. Bush endorsed the idea of a Palestinian state. Two days later, Prime Minister Ariel Sharon warned Washington not to “try to appease the Arabs at our expense.. .Israel will not be Czechoslovakia.” The administration listened. Regime change on the West Bank became more attractive than taking on Israel’s Likud government and its allies in Washington.

Since World War II, the Arab world has been largely shaped by transient passions, notably anti-colonialism, nationalism, socialism, and Islamism. The single constant, apart from corrupt and/or incompetent regimes, has been the Arab-Israeli conflict and a perception throughout the region (and most of the world) that Washington shares responsibility with Israel for the plight of the Palestinian people.

In his speech last week, Mr. Bush offered some hope, saying that if “the terror threat is removed and security improves,” Israel “will be expected to support the creation of a viable Palestinian state.. . As progress is made toward peace, settlement activity in the occupied territories must end.”

However, Mr. Bush provided no specifics. Who will judge whether the terror threat

has been removed or sufficient progress toward peace has been made? A skeptic would say that if the recent past is any guide, Israel's Prime Minister, Ariel Sharon, will make those calls. On April 4 last year Mr. Bush said, "enough is enough." And he added, "I ask Israel to halt its incursions into Palestinian-controlled areas, and begin the withdrawal from those cities it has recently occupied. Israeli settlement activity in occupied territories must stop. And the occupation must end through withdrawal to secure and recognizable boundaries." Mr. Bush also announced that he was sending Secretary Powell to the Middle East to push for a political settlement.

Two days later, Mr. Bush called Sharon and said Israel must pull its forces out of the West Bank "without delay." And the White House appeared to support Secretary Powell's idea of bringing the parties together in a peace conference. Then, Powell left on a six-day trip to the region, and General Anthony Zinni, Bush's special envoy for the Middle East, conveyed to Sharon Bush's call for Israel to withdraw at once from Palestinian cities.

On April 9, three days after the call from The President, Mr. Sharon said that Israeli would press on with its offensive in the West Bank.

On April 17, Powell returned without the cease-fire he had been seeking and unable to secure a withdrawal of Israeli forces from the West Bank. Meanwhile, An Fleischer, the White House press spokesman, was stressing that Sharon was "a man of peace.

The tilt toward Sharon reached a peak of sorts on June 24, 2002, when Bush told the Palestinian people that they would have to replace Yasir Arafat as their leader before Washington would support an independent Palestinian state. Without mentioning Arafat by name, the President made his meaning clear: "Peace requires a new and different Palestinian leadership so that a Palestinian state can be born," he said. Until then, Mr. Bush had resisted the

Sharon position—that no negotiations could take place until Arafat was gone. Polls on the West Bank have shown that Arafat's approval rating has steadily declined in recent years. It spikes, however, when he is attacked by Sharon. They appear to need each other.

Again, in last week's speech, Mr. Bush made the case that regime change in Iraq would provide the conditions for weakening terrorism and helping Palestinians achieve democracy. I disagree. The case for and against attacking Iraq now is complex. It should not be tied into the campaign against terrorism. The connection between Iraq and terrorism is at best tenuous. Most of the people I know who have followed the affairs of the Middle East over the years would argue that the single, unchanging precondition for regional peace and stability is measured but steady progress toward a settlement of the Palestine issue, starting with an end to Israel's occupation of the West Bank.

If the U.S. gets too far adrift from reality in the Middle East the sole beneficiary would be Usama bin Laden and his legatees (if UBL is dead). Their purpose - indeed, their *raison d'être* - is to divide the West from Islam, starting with the Arab world.

In the Persian Gulf, the Iranian government reacted to 9/11 by authorizing American search-and-rescue operations on its soil, the transit of humanitarian assistance and cooperation in the formation of the new Afghan government. In many Iranian cities, there were meetings to express sympathy for the victims of the attacks on the U.S. Both hard liners and reformers denounced the attacks. And at that pivotal moment, Iran's reformist government would probably have been politically free to extend its reach to America even further. The combination of sensible steps by Washington on the Arab-Israeli front and improved U.S.-Iranian relations

would have further isolated Iraq politically within the region and hence appealed to all side. But the administration's harsh reaction, notably the President's "axis of evil" remark, damaged prospects for beginning to repair a bilateral relationship with Iran of surpassing strategic importance.

Pakistan, a nominal ally, is the country that most nearly fits the President's profile of evil. Two of its provinces are controlled by Taliban and al Qaeda sympathizers. Although the issues that divide Iran and Pakistan have never reached the level of crisis, relations have worsened in recent years. Pakistan's heavy involvement with the Taliban is partly responsible. The Taliban is a bone in Iran's throat. Pakistan's Islamic schools, the *madrassas*, have become training grounds for terrorist and other radical groups in much of the Muslim world.

For now, there may be little that the Musharraf government can do about the chaos and anarchy in parts of the country. But it can and should be held to account for its remarkable decision to make possible North Korea's highly enriched uranium program. Pakistan is known to have provided much or most part of the program: weapons design; gas centrifuges; materials to make centrifuges; data of the sort that would enable the customer to avoid having to test its devices. The two-way traffic between Pakistan and North Korea, involving ballistic missiles and nuclear weapons technology, could have a dangerous ripple effect.

The campaign against terrorism generated a sense of common purpose, but at another deeper level, also became divisive. Most of Mr. Bush's advisors regard the first and best answer to threats to security as lying in preponderant military force. European governments, along with most others, see military force as a complementary tool in the campaign against terrorism—less essential than a soft-power mix of intelligence, law enforcement, border and financial controls. Terrorism is generally seen as part of a larger problem, not a single problem. Thus far, however, the administration's concern with the causes of terrorism has been minimal.

Its focus instead has been on identifying and destroying the terrorist threat "before it reaches our borders," if necessary acting alone and using preemptive force." This thinking is contained in the novel doctrine laid down by the administration last September.

Other governments assume, doubtless correctly, that in its reliance on massive military power, the new doctrine downgrades alliances. They also worry that the administration may not feel bound by the body of international rules and restraints that developed after World War II. Taken at face value, the new doctrine justifies preventive war waged without allies and without U.N. sanction.

A doctrine of preemption that relied on very high quality intelligence to identify an impending attack well in advance and then head it off would not raise eyebrows. But the Bush doctrine is based instead on prevention and preeminence-- that is, taking military power to a level never before seen—one that would so intimidate all parties that no one would even consider an attack of any kind against the U.S. Threats to U.S. interests would be not just discouraged but precluded. "Full spectrum dominance," was a term for it in Defense Department circles.

This visionary theory should be seen for what is-- a doctrine of preventive war. Mr.

Bush himself stated it clearly in a speech at West Point in June, 2002: “We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge.”

“Anticipatory self-defense” is a phrase that Secretary Rumsfeld has used. The notion of regime change is the other side of the coin.

In practice, such a doctrine harbors many risks. It exaggerates the role and utility of raw military power. The government could find itself unable to carry out programs in other realms—unable, for example, to cooperate effectively with other governments to combat terrorism. Special forces and smart weapons can help in that battle, but other tools, starting with good intelligence and good police work, are more important.

No matter how good the performance of the intelligence community, surprises are probably unavoidable. Thus, measuring performance by the standard of prediction is unrealistic and can damage the standing, morale and performance of intelligence agencies. They are engaged not in winning a war against terrorism but in managing it—restricting the activities and options of hostile forces. The Bush doctrine, if taken seriously, would mean that prediction would become the measure of performance, because a prevention-based strategy would require sustained and timely collection of the kind of intelligence that is rarely available, least of all in a form that connects all the dots.

Effective intelligence collection must be conducted bilaterally but with a wide array of countries. After 9/11, offers of help, large and small, poured in to Washington from around the world. They were rejected, another opportunity lost. Accepting these offers would have harmed nothing, generated enormous good will, and, most important, helped at another, more important level. What the U.S. has needed from other countries, then as now, is information— a process through which intelligence may be shared with countries best equipped to penetrate terrorist

organizations and cells. Many of these countries took part in the sanctions against Iraq, and most of them have experienced serious difficulties of one kind or another with the terrorists groups located in the extensive region they share.

Terrorism may be contained if intelligence services and police agencies acquire the habit of cooperating closely with each other and suppressing their competitive instincts and preference for acting alone. The United States would be the chief beneficiary of such activity, first because it appears to be the primary target of al Qaeda and sibling terrorist groups; second, because it lacks adequate human resources for gathering the intelligence it needs; and third, because its ability to eavesdrop on global communications is declining. The rapid growth of commercially available technology is reported as allowing for the creation of all but unbreakable computer codes. Fiber-optic lines give off no electronic signals that can be monitored.

John Newhouse is a senior fellow at the Center for Defense Information, Washington, D.C. An expert on arms control and diplomacy, he served as a senior policy advisor on European affairs in the State Department from 1998 to 2001. He is the author of Europe Adrift and War and Peace in the Nuclear Age, and the coauthor of Assessing the Threats, CDI, 2002.



The Threats America Faces

John Newhouse

Before September 11, the threats from weapons of mass destruction and terrorism were treated for the most part as ugly abstractions and not likely to materialize, even though they had done so in the recent past. Now we recognize the threats as being all too real but difficult to assess in terms of their imminence and gravity. There are too many unknowns and uncertainties. What does seem clear is that the major source of the threat has changed. State-sponsored terrorism has steadily declined in recent years.¹ However, the incidence of acts by nonstate terrorists has risen.

Both the Clinton and Bush administrations elected to stress a highly implausible threat to the territorial United States from unfriendly regimes, notably North Korea and Iran. Early in 2001, the State Department conveyed the official line in a guidance memorandum to embassies: "The principal threat today is...the use of long-range missiles by rogue states for purposes of terror, coercion, and aggression."²

This dubious proposition—an article of faith within parts of the defense establishment—obscured existing and far more credible threats from truly frightful weapons, some of which are within the reach of terrorists. They include Russia's shaky control of its nuclear weapons and weapons-usable material; the vulnerability of U.S. coastal cities and military forces stationed abroad to medium-range missile systems, ballistic and cruise; the vulnerabilities of all cities to chemical and biological weapons, along with so-called suitcase weapons and other low-tech delivery expedients. Vehicles that

contain potentially destructive amounts of stored energy are a major source of concern, as is one of their most attractive potential targets, a nuclear spent-fuel storage facility.

The example set by youthful Palestinian belt bombers can and very possibly will be emulated by terrorists elsewhere, including the United States. Preventing human bombs is "an incredibly difficult business," says Christopher Langton, an authority on terrorism at the International Institute of Strategic Studies. "It's cheap," he says. "It has the most accurate guidance system available to mankind. It is easily concealed."³

The companies that generate, transmit, and distribute electricity are thought by many to be a more serious potential target. The computers that control the nation's electric power system have apparently been probed from the Middle East, and terrorists may have even inspected the physical equipment.⁴

Many experts argue that information warfare directed against air traffic control, the banking system, and communication satellites constitutes a broad and more persistent threat than those associated with weapons of mass destruction (WMD). Some would add environmental issues and narco-trafficking to the list, and ask whether advocates of deploying weapons in space have begun to contemplate the potentially troublesome ripple effect of movement in this direction.

The Bush administration states, wrongly, that the threat from ballistic missile systems is spreading. In fact, there are fewer such systems in the world than 15 years

ago, and fewer nations are trying to develop them. Most of the countries that deploy ballistic missile systems have friendly relations with the United States and possess short-range systems that could only threaten neighboring states.⁵

Even the latest National Intelligence Estimate notes in its summary that the United States "is more likely to be attacked with materials from nonmissile delivery means—most likely from terrorists—than by missiles." The nonmissile alternatives, the report says, "are less costly, easier to acquire and more reliable and accurate. They can also be used without attribution."⁶

Obviously, there is no wholly reliable or seamless protection against the use of WMD by terrorists. Probably more important than any of the active defenses, which are as varied as the weapons they are designed to neutralize, is the overarching need for prior restraint, which is also known as passive defense and is based on agreements between nations. Some of these agreements set limits on destructive weapon systems. Others turn on preventive diplomacy, still others on exchanges of surveillance data and military transparency. Some of the agreements are bilateral, others the product of diplomacy conducted under the auspices of, yes, multilateral institutions.

Traditional measures can be used to manage the conflict that began last September. Prior restraint, imbued with an especially heavy infusion of creative but patient diplomacy, can become the decisive weapon for waging what could be called the "hidden hand war." We may not know who exactly the adversary is, where exactly he is located, or the extent of his capacity to create havoc. And this conflict may not reach a conclusion. The enemy, if neutralized, may go to ground and reappear one distant day.

Smart weapons and military superiority may dictate the course of a given battle but will not affect the outcome of a campaign against a worldwide web of amoeba-like terrorist cells. The performance of government

and the military in this conflict will be no better than the intelligence to which they have access, much of which can only be gained through the give-and-take of diplomacy. Rarely in its past has the United States been obliged to rely so heavily on the cooperation of other states.

Weapons of mass destruction diverge greatly in the destructive power they can unleash. Nuclear weapons aside, few such weapons would be likely to take as many lives as were lost on September 11. An attack, say, with biological and/or chemical weapons could, in theory, take that many or more but would probably fall far short of that number. The destructive effects of even a primitive nuclear weapon would, by contrast, vastly exceed any other horror that could be imagined. Moreover, there is no more serious threat from WMD than the several uncertainties that nuclear weapons have created. And the most acute of these is the possibility of a weapon being launched by accident or inadvertence—by Russia or the United States.

Russian Weapons

The implicit threat to the United States from Russia's nuclear edifice is more acute than it was during the Cold War. Control of Russia's fissile material is far from adequate, let alone reliable. Russia's early warning network is deteriorating. We know that the General Staff still controls the launch codes. But there are reports from authoritative sources about the declining competence of missile-control crews, their lack of training, and the increasing stress imposed by the thousands of nuclear weapons deployed on hair-trigger alert. Senior officers in Russian nuclear forces talk of spending half their time dealing with the stress and strain on their people.

The State Department's 2001 guidance memorandum, which cited rogue states as the principal menace, was preceded by the report of a bipartisan task force led by former Senate majority leader Howard Baker

and former White House counsel Lloyd Cutler that took a different view, and concluded: "The most urgent unmet national security threat to the United States today is the danger that weapons of mass destruction or weapons-usable material in Russia could be stolen and sold to terrorists or hostile nation-states and used against American troops abroad or citizens at home." The report warned of delays in payments to guards at nuclear facilities; breakdowns in command structures, including units that control weapons or guard weapons-usable material; and inadequate budgets for protection of stockpiles and laboratories.⁷ It cited "impressive results so far" in current nonproliferation programs but concluded that if funding were not increased, there would be an "unacceptable risk of failure" that could lead to "catastrophic consequences."⁸

Helping Russia to arrest the decline in the safety and security of its nuclear weapons and materials has not been but should become a carefully coordinated three-step approach. Step one would be to assign custody of all weapons-grade fissile material to the Ministry of Atomic Energy, eventually disposing of it. Step two would be to assign custodial responsibility for storage of nuclear weapons to the Ministry of Defense. Step three would amount to removing both Russian and American nuclear missile systems from a quick-launch posture by de-alerting them and moving the warheads to storage (step two) en route to dismantling and disposal (step one).⁹

There are known to be 1,000 tons or so of highly enriched uranium and 150 tons of plutonium scattered around Russia, much of it in badly secured storage sites.¹⁰ There may be even more such material, and not all of the storage sites have been identified. In any case, it is enough material, according to Sen. Carl Levin, chairman of the Senate Armed Services Committee, for between 60,000 and 80,000 nuclear weapons; or, as he observed, enough to constitute "a proliferation nightmare."¹¹

Discouraging the theft or illicit sale of Russian materials will require more support for the appropriate steps. The most important of these are the Nunn-Lugar cooperative threat reduction programs named for their founders, Sen. Richard Lugar and former senator Sam Nunn. These programs aim to consolidate and ensure the security of the Russian materials. The Baker-Cutler report recommended a three-fold increase in funding to \$3 billion annually for these programs.

But the effect of additional spending may be at least partially nullified by the agreement on limiting deployed warheads that Presidents George Bush and Vladimir Putin signed in Moscow at the end of May. The text was both meager and indulgent. Russia got what it (and the U.S. Senate) wanted—a binding agreement in treaty form. The Bush administration got what it wanted—a deal that won't inhibit any part of the Pentagon's strategic planning. Not a single missile launcher or warhead will have to be destroyed or disabled under the agreement. Each side can carry out the reductions at its own pace, or even halt reductions and rebuild its forces. Briefly, the United States gets a "reconstitution capability," as it's called, as a hedge against threats that may one day be posed by China or a retrograde Russia.

An escape clause allows withdrawal on three months' notice. The only constraint is that each side can have no more than 1,700 to 2,200 weapons at the end of 2012, when the treaty expires. And those are the numbers called for by the Pentagon in its Nuclear Posture Review. Also, at the end of 2012, each party is free to deploy as many weapons as it chooses unless the agreement is extended.

Since the deactivated warheads will be moved into storage facilities instead of being disabled, they can remain as targets for terrorists. But that danger, it has been argued, is more apparent than real since terrorists are presumably less intent on trying

to steal a large, strategic weapon than a much smaller, tactical one, of which there may be many more—most of them in Russia. We don't know how many. Estimates vary from between 4,000 and 15,000, and besides being more portable, these weapons are thought to be less protected by computerized anti-use codes. Nor can we be sure about the quality of security in some of the warehouses in which these weapons are stored or whether Russia can afford to provide adequate security. What does seem clear is that if the Moscow agreement had provided for destruction of strategic warheads, a useful precedent would have been set. The logical follow-on step could have been a negotiation aimed at getting rid of all or most of the tactical weapons in storage. Politically, the Moscow agreement is another step toward strengthening the U.S.-Russian relationship. However, it will have little, if any, bearing on the interconnected threat of weapons of mass destruction and terrorism.

Less attention has been devoted to the related and possibly graver question about Russia's capacity for preventing a nuclear weapon being launched by accident or inadvertence. The problem, although complex, stems from a generalized decay of the military infrastructure brought on by diminishing resources. Russia's increasing dependence on nuclear weapons as its conventional forces shrink as a result of budgetary pressures sharpens the concern, especially since its long-range missile forces are themselves in a virtual free-fall. Since the 1980s, there has been a 56 percent decrease in Russian missile systems capable of striking the United States and a 48 percent decrease in the number of warheads deployed with these systems.¹² This downward trend is likely to reinforce the concerns of Russian planners that their diminishing strategic deterrent could be neutralized by America's superior offensive forces.

Russia's strategic forces are judged to be more vulnerable than at any time since the

early 1960s. Operational problems bedevil Russia's surveillance/early-warning system. A fire at a satellite control station earlier this year is believed to have crippled space-based components relied upon to detect a missile attack. The system was already in serious disrepair. Whereas the comprehensive early warning network operated by the United States would detect any significant attack from Russian missiles, Russia's more limited system left behind by the Soviet Union is considered to be incomplete and unable to provide continuous or comprehensive surveillance of attack corridors.¹³ The Congressional Budget Office and various authorities have warned that most of the Russian satellites have reached the end of their lives and are drifting out of control.

Russia's warning system against submarine missile attack, designed around a new generation of satellites, is still inoperable. According to one authoritative estimate, the U.S. Navy's Pacific-based Trident submarines, armed with the powerful and highly accurate D-5 missile, would be able to launch attacks through the Pacific gap in Russia's ground-based radar.¹⁴

A warning system as flawed as this one has already shown itself to be susceptible to false alarms and close calls. As Bruce Blair, president of the Center for Defense Information in Washington, D.C., has written, "a degraded early warning network loses some of its ability to screen out false indications of attack generated by the sensor network. A broken communications link may delay the transmission of a legal launch order, but it may also degrade safeguards against an illegal launch. To illustrate, the special nuclear command link running from the General Staff in Moscow to the launch crews in the field enables the General Staff to quickly transmit the go-code, but it also provides a feedback loop from the missiles to the General Staff to detect and prevent any unauthorized launch attempt at any subordinate level of command. Any number of examples of

this simultaneous erosion of positive and negative control could be provided.¹⁵

A variant of the unthinkable accident is a scenario in which a medium- or short-range missile—ballistic or cruise—aimed at an American or Russian city is launched from a ship by a terrorist group and, in the ensuing confusion and uncertainty, the targeted nation initiates a nuclear exchange against the other. Avoiding an event more serious than a close call is the driving task that Washington and Moscow are not treating as urgently as they should, or indeed with any urgency. There is wide agreement that the first step should be the de-alerting of American and Russian strategic missiles. Thousands are deployed on silo-based missile launchers and on submarine-launched systems and kept on hair-trigger alert. De-alerting means separating the missile warheads from launchers and thereby all but removing the danger posed by this quick-launch posture.

The step cannot be taken unilaterally, and bilateral movement will be difficult given the pressure on Russia to sustain the credibility of its diminishing strategic forces by keeping a major portion of them on alert status. But de-alerting may be altogether ruled out by Moscow if it views these forces as being made vulnerable by a convincing American decision to go forward with National Missile Defense (NMD). Russian planners might well regard the combination of America's superior offensive forces and NMD as neutralizing their country's nuclear deterrent.

Actually, the recent Moscow summit offered a plus, probably unintended. Warehousing roughly two-thirds of the deployed warheads will amount to a long, de facto step toward de-alerting the forces.

An agreement to share information on the launch of ballistic missiles is another step waiting to be taken. An agreement on joint missile surveillance was signed in September 1998 by Bill Clinton and Boris Yeltsin. Predictably, the bureaucracies on

both sides were unprepared for collaboration in an area so sensitive. In June 2000, however, Clinton and Russian president Vladimir Putin agreed to move matters along by creating a Joint Data Exchange Center (JDEC) in Moscow. Its purpose would be "to ensure the uninterrupted exchange of information on the launches of ballistic missiles and space launch vehicles."¹⁶ Six months later, the lame-duck Clinton administration reached an agreement with Russia that set forth in detail how the JDEC would operate. And there matters rest. The Bush administration has thus far shown no interest in JDEC.¹⁷ Still, events may create an interest. And JDEC could be very useful, perhaps more so than any step yet envisaged, with the exception of de-alerting, the absent cornerstone of accidental launch prevention.

Pakistan's Nuclear Weapons

The war against al-Qaeda and its Taliban host has pointed up disturbing uncertainties about Pakistan's nuclear weapons. We know too little about them, and we hear divergent views from people with special knowledge of the problem. We do not know exactly how many weapons Pakistan has deployed; estimates based on somewhat sketchy information point to 35 or so. Nor do we know where some of them are stored or whether weapons are stored separately from delivery vehicles. Exactly who in Pakistan possesses that knowledge, including the whereabouts and security of fissile material, is also unclear. Pakistan is secretive because it worries that external forces, starting with India, might want to take control of or destroy its nuclear weapons.

A widely but cautiously held view is that the weapons themselves are secure so long as Gen. Pervez Musharref's government can prevent upheaval and remain in power. Another rather widely held but equally cautious view is that the government has staying power. Still, it has not inspired confidence, and what would happen in the event of its overthrow is the major uncertainty,

hence a major concern. Inevitably, there has been talk of "exfiltrating" Pakistan's nuclear weapons in that event, a possibility that most people with special knowledge regard as implausible. Former deputy secretary of state Strobe Talbott has said, "I doubt that we know where everything is that we would be going to exfiltrate or extract—[and it would be] dangerous because it would almost by definition be in conditions of political instability when there would be a lot of potential for violence."¹⁸

Whether even terrorists with a background in nuclear technology could activate a Pakistani nuclear weapon is unclear. Pakistan's weapons, unlike America's and Russia's, are presumed to lack devices of the kind that prevent warheads from being armed unless various codes are punched in. Some U.S. officials have spoken of transferring such devices to Pakistan in order to enhance the security of the weapons. Others oppose such a step, arguing that it would encourage Pakistan to deploy weapons now kept in pieces for safekeeping. Instead, the argument runs, the United States should help only by providing better surveillance equipment, thereby improving physical security around Pakistan's nuclear weapons sites.¹⁹

Dirty Bombs

Terrorists may discover, or have already discovered, that a usable nuclear weapon is beyond their reach. That is the cautious view of many, though not all, specialists. A more attainable alternative, however, might be the so-called dirty bomb, a radiological device using chemical explosives to contaminate a targeted area for an extended period. Various accessible materials could be used to make such a device, including radiological medical isotopes. Another source might be spent fuel rods, although these are highly radioactive, heavy, and difficult to handle.²⁰

Exposure to toxic radioactive material would be harmful or fatal to some humans and, depending on location, might also con-

taminate livestock, fish, and food crops. Terrorists, too, would confront safety risks; turning radioactive material into a bomb and delivering it to the target could be dangerous at every stage. Nonetheless, covert disposal of radioactive materials would create widespread alarm and confusion, at the least by planting well-founded concern about long-term increases in the cancer rate. In short, the dirty bomb should not be regarded as a weapon of mass destruction, but as one that if used would cause mass disruption.

After September 11, the Nuclear Regulatory Commission began to consider buying millions of doses of potassium iodide, a drug that protects against thyroid cancer, which can be caused by exposure to radiation. In 1988, the commission decided to offer the drug free to states wanting to stockpile it, but it rescinded the offer the following year. A problem with potassium iodide as a remedy is that it must be given prior to radiation exposure, or shortly thereafter, which means that it must be stored near the site of potential exposure.²¹

The Defense Department suggests that with prompt detection most external agents could be disposed of by removing outer clothing and shoes. But prompt detection of covertly dispersed radioactive material can hardly be relied on. Also, just which agencies would be responsible for detection, treating the injured, and discouraging panic is unclear. The public health authorities are simply not prepared to deal with the radiological effects of either a dirty bomb or an attack against a nuclear plant.

Biological and Chemical Weapons

Biological and chemical weapons have been the focus of much of the informed discussion about weapons of mass destruction, partly because anthrax has already been used, and partly because the United States is unprepared to prevent or cope with a large-scale attack using such agents. The U.S. Public Health Service is especially vulner-

able. It was gutted in the 1980s, and has since been neglected. "We recognize that we have not as a country, nor as a District, nor as a state, invested the necessary scarce resources in our local and state public health systems," Secretary of Health and Human Services Tommy G. Thompson said in a news conference this past January.²² According to various public health experts, about 10 percent of local public health departments do not have e-mail, and about 40 percent lack high-speed internet access.²³

Stockpiles of vaccines for various pathogens, if they exist at all, are very small. The United States possesses just 15.4 million doses of smallpox vaccine. These will be diluted to raise that number to 77 million doses. A contract signed in November 2001 with a U.K.-U.S. pharmaceutical partnership could yield 285 million doses by the end of 2002—enough to cover the entire population. But the vaccine is still in the early stages of clinical trials.²⁴

The administering of anthrax vaccine involves six painful shots that make many people sick, and specialists at the Center for Disease Control in Atlanta are not even sure that the vaccine protects against the strain of anthrax that was used against members of Congress and the news media last fall.²⁵ However, an improved one-shot version is well within reach of the pharmaceutical industry. Last January, the U.S. Food and Drug Administration released over 200,000 doses of the current vaccine. The Defense Department "welcomed" this action but did not commit to further vaccinations of military personnel, announcing only that it expects to reach a decision on whether to do so "in the near future."²⁶

The healthcare system would be quickly overwhelmed in the event of a high-casualty attack in which bio-chemical weapons were employed. Hospitals would not have adequate emergency treatment facilities. Victims of contagious diseases could appear in waves, and the symptoms of such diseases as smallpox, which would need to be contained

before becoming epidemic, might not be immediately recognizable by many or most doctors.

Perhaps the most immediate and acute threat from toxic chemicals is a terrorist assault on a plant that manufactures them. A recent study by the army's surgeon general concludes that as many as 2.4 million people might be killed in an attack on a toxic chemicals plant if it were located in a densely populated area. Even the mid-range estimate is for 900,000 casualties.²⁷

Fortunately, producing, sustaining, and dispensing biological and some chemical agents would confront nonstate terrorists with major risks and difficulties. Attempts to encapsulate, or weaponize, a deadly virus are likely to render it dysfunctional. Moreover, the chances are that a terrorist bent on martyrdom would die before the complex task of dispensing the weapon was actually completed.

Biological weapons fall into several categories. These include bacteria, which cause such diseases as plague and anthrax, and viruses, which cause smallpox and Ebola. Most bacterial infections can be treated with antibiotics, provided the problem is identified at an early stage and enough drugs are available.

However, not much else can be said with certainty. Whether the most lethal agents could be used on a scale sufficient to kill thousands of people, or even hundreds, is a question on which informed opinion divides sharply. "Low probability, high consequence" is probably as good a characterization of the threat as any.²⁸

The example of Aum Shinrikyo, the Japanese terrorist cult, may be instructive. In 1995, Aum Shinrikyo tried to kill thousands of people, first by developing and dispensing various germ weapons, including anthrax. These efforts were a total failure. Next, the group tried reaching its goal by releasing sarin, a deadly nerve gas, in Tokyo subways. In the end, 12 people died, and roughly 5,500 were affected, most of them

mildly. The cult was unable either to produce high-purity sarin or dispense it effectively. What some analysts concluded from this experience was that states bent on causing mayhem could overcome the operational challenges presented by biological agents and some chemical warfare agents but sub-state terrorists probably could not.²⁹

To date, the discussion of the threat from biological and chemical agents has dwelt too little on the difficulties and dangers of employing the various agents to serious effect. Scholars and policymakers have indulged in extreme thinking about this form of terrorism, according to Jessica Stern, the author of *The Ultimate Terrorists*. "Until recently," she notes, "the threat was entirely ignored; now, it is attracting too much frenzied attention and too little careful analysis, inspired by a widespread conviction that the *Aum Shinrikyo* case proves that [such] attacks resulting in hundreds of thousands of deaths are all but inevitable. Both attitudes are dangerous. The first has led to the underfunding of programmes designed to prevent or mitigate the threat. The second is leading to over-reaction and hasty decisions, some of which will harm international security."³⁰

Temperature, sunlight, wind, and moisture can all prevent effective delivery of chemical weapons. Biological pathogens are living organisms and thus more fragile than chemical agents. Chlorine in the water supply can kill them. Munitions can as easily vaporize an agent as dispense one. If released from a bomb or warhead, explosive effects would destroy all but 1–2 percent of the agent.³¹

A terrorist group with links to a state already in possession of bio-chemical weapons could be a serious threat. Otherwise any such group, even if well funded, would probably be unable to inflict mass casualties by dispensing one of these weapons. Still, they are instruments of terror and, as shown by Japan's reaction to Aum Shinrikyo's deadly enterprise, even an attack that

fell far short of its goal can produce a reaction lying somewhere between alarm and panic.

Cruise Missiles

Improved guidance and propulsion technologies, some of them off the shelf, are producing a variety of new threats, or more intimidating variants of existing ones. Cruise missiles offer an especially strong example. In the past decade, they were considerably more available, more usable and put to greater use than ballistic missiles.³²

Cruise missiles can be launched from a wide array of land- or sea-based platforms as well as from manned or unmanned aircraft. Unlike ballistic missiles, cruise missiles have wings, are propelled by jet engines, and never leave the Earth's atmosphere. They can be adapted to increase their range much more easily than ballistic missiles. Range can be extended by a factor of five or more without altering the system's airframe or engine. They are smaller and a lot cheaper than ballistic missiles. Compared with ballistic missiles, America's Tomahawk cruise missile, for example, which is 18 feet long and 21 inches in diameter and weighs 3,200 pounds, resembles a toy. In contrast, the intercontinental MX missile system weighs 100 tons and is 70 feet long and nearly 8 feet in diameter.

Cruise missiles are hard to detect, and newer versions are incorporating stealth technology. With or without this technology, they are far more accurate than ballistic missiles, capable of striking within a few feet of the target; longer-range versions become preemptive weapons. In all versions, cruise missiles are better suited than ballistic missiles for delivering chemical and biological weapons.³³

They pose a number of problems, the first of which is proliferation. The incentive for governments to acquire cruise missiles, especially the land-attack version (LACM), is strong because even building a significant number is cheaper than creating a modern

air force. Many of the components that go into cruise missiles, unmanned aerial vehicles (UAVs), and commercial aircraft are common to each.

There are various ways of building a force of cruise missiles, none of them especially difficult.³⁴ Procuring complete systems from a supplier state is the most direct route, but buyers may run up against the Missile Technology Control Regime (MTCR), an informal export control association of 33 countries that was set up to inhibit the spread of ballistic and cruise missiles and, more recently, chemical and biological weapons. The MTCR membership includes the major suppliers of advanced missile systems and subsystems. The members operate under a set of guidelines; however, there are neither enforcement provisions nor sanctions for violations.³⁵

The MTCR and other restraining ordinances are unlikely to deter supplier countries determined to sell dual-use aircraft and cruise missile components to other countries. Indeed, the MTCR excludes manned aircraft. And, as noted in a recent report published by the Carnegie Endowment for International Peace, "as large UAV's evolve for reconnaissance, missile launching and even civilian communications, pressures are growing to relax MTCR restrictions. Given the likely importance of unmanned combat air vehicles (UCAV's) and other UAV's in the Bush Administration's military strategy, these issues will come to the fore very soon."³⁶

Many countries are putting their development programs underground so as to hide them from overhead intelligence systems. For that and other reasons, the extent of cruise missile proliferation is far from clear.³⁷ A few of the countries that, ideally, should be part of the Missile Technology Control Regime, including China and Israel, are not. China has been developing land-attack cruise missiles for 20 or so years, and Israel is en route to becoming a major player in the cruise missile stakes.³⁸ India, which has

not joined the regime either, recently tested a supersonic, medium-range cruise missile, an event described by *Defense News* as "just one of the fruits of a secret joint research agreement between India and Russia."³⁹ And Russia is one of a number of club members whose adherence to the MTCR guidelines is suspect.

Building cruise missiles around components available on the world market is nearly as simple as procuring complete systems. Most of the relevant technologies are dual-use; the few exceptions, including advanced propulsion systems for long-range LACMS, continue to be restricted. For many years, advanced guidance systems, such as Terrain Contour Matching (TERCOM), were tightly controlled, but their importance receded in the early 1980s when the Global Positioning System (GPS) became widely (and freely) available.⁴⁰ The easy access to GPS and inertial guidance systems has enabled some states to gain a 15-year head start in navigation with a single purchase. (Some of the states that are nearing or crossing these frontiers of technology can neither feed the mass of their people nor provide them with health care or other basic needs.)

The intelligence community worries about proliferation of land-attack cruise missiles. Vice Admiral Thomas Wilson, director of the Defense Intelligence Agency, has said as much: "The potential for widespread proliferation of cruise missiles is high.... Major air and sea ports, logistics bases and facilities, troop concentrations, and fixed communication nodes will be increasingly at risk."⁴¹ Modern cruise missiles can be programmed to attack a target simultaneously from different directions, overwhelming air defenses at their weakest points. Also, LACMS can fly circuitous routes toward a target, thereby avoiding radar and air defenses.⁴² The stealth technology will make cruise missiles even more formidable.

Specialists inside and outside the intelligence community have worried over the years about a major threat from cruise

missiles. It has not yet emerged on the scale foreseen, but it will. And efforts to control the number and versatility of cruise missiles may be largely unavailing.

Rogue State Weapons

The acute dangers described in the foregoing have consumed far less of Washington's attention than the exhaustively debated threat of an intercontinental ballistic missile (ICBM) purposely launched against the United States by a rogue state. This political dynamic created the pressure to develop a missile defense system against the threat and kill the Anti-Ballistic Missile Treaty. This current of opinion is strong but misguided. The missile programs of Iran and Korea are part of a deterrent strategy directed primarily against traditional enemies. For example, Iran's missile systems, when deployed, are likely to be targeted against first Iraq and then Israel, Saudi Arabia, and the U.S. forces deployed in the region.

North Korea is the only one of the five designated rogue states with a missile development program that has made measurable progress. Indeed, the perception of an increasing ballistic missile threat to the United States derives almost entirely from the missile program and exports of North Korea.⁴³ Among the other four so-called rogue states—Iran, Pakistan, Iraq and Libya—only Pakistan is judged to have succeeded in developing nuclear warheads for its missiles. Iran's missile systems, the Shehab-3, with a range of 600 miles and the Shehab-4, with a range of 900 miles, are knockoffs of North Korea's No-Dong missiles, a system that has tested badly. Pakistan's only mid-range system, the Ghauri, with a range of 900 miles, was also spun off from the No-Dong program.

Whether North Korea can or will want to continue supplying technology and parts to Pakistan and especially Iran is not clear and may depend on what becomes of efforts to revive the discussions between Washington and Pyongyang aimed at shutting down

the North Korean programs. The talks had gone a good distance under the Clinton administration before being frozen by President Bush. The intelligence community is sensitive to and, not for the first time, intimidated by the political current. Only the State Department's intelligence people dissented from the assessment naming North Korea and Iran as near-term threats to the United States.

North Korea may be tempted to try to build an extended-range version of the three-stage Taepo Dong II that could reach parts of the western United States. The current version of the system has yet to be tested, however, and technological hurdles could block efforts to go further. The political effects of North Korea's program will probably have more lasting importance. There will be a continuing confrontation with Washington so long as the program exists, largely because of North Korea's exports to other worrisome states. Almost certainly, however, the program exists to be bargained away in return for concessions, economic and political, from Washington. Pyongyang's implicit message to President Clinton's negotiating team, boiled down, was: you want us to give up earning money with our missile exports, then offer assistance and improved relations. While there has been no let-up in North Korea's research and development programs, Kim Jung Il, on a visit to Moscow in July 2001, promised that there would be no flight testing of any of his missile systems before 2003. He offered this pledge unconditionally.

If North Korea were to sell the Taepo Dong II, which has never been tested, to Iran or Pakistan, Washington's concern would grow sharply, although neither Iran nor Pakistan would be able to strike Alaska or the mainland United States with this system. The Central Intelligence Agency has maintained that deployment of an ICBM is a first priority for Iran. The missile would presumably be the longer-range version of

the Taepo-Dong II that is still largely a paper system. Although Iran disavows any intention of developing a system of greater range than the Shehab III, some of the signs suggest otherwise. The real question is whether Iran could or would be able to finance the development of a strategic missile program over a necessarily long period. The answer is far from obvious. Meanwhile, efforts to develop the Shehab III, a vastly simpler system than any ICBM would have to be, are proceeding, but with mixed results.

Most of the Clinton administration's national security apparatus, according to a *New York Times* report, feared a more imminent danger than the one portrayed by the CIA and others. "The intense focus on long-range missiles that could hit American soil also obscured the more immediate threat posed by nuclear weapons carried by terrorists or fired from ships. The officials said the change in focus devalued the concept of deterrence, by which the sheer force of the American arsenal would inhibit even the most irresponsible leader from attacking American soil."⁴⁴

Ironically, the documents that contributed most to inflating the threat from North Korea and Iran—the Rumsfeld Commission report of 1999 and the intelligence community's unclassified estimate of the ballistic missile threat that appeared a few weeks later—could be read as supporting a contention that Washington had radically skewed the threat. Both documents noted that the United States confronts a wide range of threats, of which the most imminent, credible, and dangerous involve not unfriendly ICBMs, but cargo ships, or other sea-based platforms, equipped with medium-range ballistic or cruise missile systems (or chemical or biological weapons) and deployed not far from the U.S. coastline. These non-ICBM systems were described by the intelligence estimate as being less expensive to develop, easier to produce, more easily disguised, and probably more

accurate than ICBMs for at least the next 15 to 20 years.

In August, Tom Daschle, the Senate Majority Leader, recommended taking \$2.5 billion from the administration's funding request for National Missile Defense and using the money to develop defenses against what he called the more immediate threat from cruise missiles and theater ballistic missiles. At this still early stage of the Bush administration, some of the threats to U.S. interests and international stability have not been thought through, perhaps partly because there has not been enough time, but partly, of course, because the war on terrorism has absorbed the administration's attention.

Lower-Profile Threats

There is an array of threats that are vastly more credible than the widely discussed notion of long-range missiles deployed by rogue states, and there are few, if any, active defenses against many of them. To take just one example, thousands of container ships, many of them carrying hundreds of containers, arrive in the United States annually. But less than 5 percent of the containers are checked by customs officials, and the identity of the packers is often unclear.

Another example is the potential for massive disruption and damage inherent in fuel trucks and other vehicles that can carry large amounts of stored energy. On any given day, about 6,000 trucks cross the bridge between Windsor, Canada, and Detroit. Half of them carry auto parts, the rest other cargo. Customs officials, who are on duty 24 hours a day, are not authorized to check these vehicles. Inspecting each truck would mean having to do so in just 15 seconds, although an adequate inspection cannot be completed in less than 15 minutes. Even checking, say, every fourth vehicle could create gridlock on the bridge, thereby disrupting the "just in time" rapid transportation system on which much of our economy depends. An agreement with Canada, signed

last December, should help. One of its provisions will allow customs officials to inspect factory shipments on site and then electronically seal the container. A similar deal with Mexico is being worked out.

The Need for Sustained Multilateralism

Nothing less than *sustained* multilateralism will enable major powers to neutralize the interactive problems of terrorism and weapons of mass destruction. As noted above, passive defense based on agreements among nations and between nations and international institutions is the only reliable means of limiting the spread of destructive weapons and discouraging their use by one state against another, whether by design or accident.

Efforts to shut down financial support for terrorist cells must be multilateral. The scope of the challenge is evident in former national security advisor Brent Scowcroft's observation that "there are thousands of avenues for the laundering of money into the terrorist organization."⁴⁵

Regarding intelligence, no matter how good the performance of the intelligence community, surprises are probably unavoidable. For that reason, measuring performance by the standard of prediction is unrealistic and can damage the standing, morale, and performance of intelligence agencies. They are engaged not in winning a war against terrorism but in managing it—restricting the activities and options of hostile forces. However, in waging this campaign the administration talks of discarding deterrence and various forms of passive defense in favor of a strategy of preemption. In that case, prediction would have to become the measure of performance, because a preemption-based strategy would require sustained and timely collection of the kind of intelligence that is rarely available, least of all in a form that connects all the dots.

Effective intelligence collection must be conducted bilaterally but with a wide array of countries. Terrorism can be contained if

intelligence services and police agencies acquire the habit of cooperating closely with each other and suppressing their competitive instincts and preference for acting alone. The United States would be the chief beneficiary of such activity, first, because it appears to be the primary target of various nonstate terrorists; second, because it lacks adequate human resources for gathering the intelligence it needs, notably in Central Asia; and third, because its ability to eavesdrop on global communications is declining. The rapid growth of commercially available technologies is allowing for the creation of all but unbreakable computer codes. Fiber-optic lines give off no electronic signals that can be monitored.⁴⁶

The United States needs help, especially from allies and other friendly regimes that have productive relationships with countries in this region and in the Middle East. (America has never been good at old-fashioned spying or penetrating the intelligence services of unfriendly countries.) The 1984 summer Olympics in Los Angeles may have produced a model of diligent cooperation among intelligence services operating at both the national and multilateral levels. Well in advance of the games, the U.S. intelligence community felt certain that the possibility of a terrorist action in Los Angeles had been virtually eliminated. Subsequent Olympic events have been equally insulated against terrorism. More impressive was what did not happen during Y2K, when planned attacks by terrorists were thwarted by the combined efforts of intelligence services.

The same could be said of the protection against terrorism that swiftly built up around members of the coalition that took part in Desert Storm in 1990–91. Joint intelligence operations conducted at the time rolled up 30 or so terrorist groups, many of them connected to Iraq. U.S. intelligence agencies found themselves collaborating with elements normally considered more or less off-limits.

The lesson is that terrorism has been headed off when the intelligence agencies of like-minded governments have ramped up cooperation, usually under the pressure of some major event. After such events, however, agencies tend to ramp down, returning to their normal "stovepipes" pattern, which is shorthand for information drifting from the lower to the upper levels of an agency's confines, but not beyond. The terrorist strike against the World Trade Center in 1993 was the consequence of ramping down.

Left to itself the intelligence community is unlikely to take this lesson to heart. Old habits die hard, and the agencies regard sharing information as compromising security. It is counterintuitive, in part because knowledge is power and possessing it may give one of the parties an edge in bureaucratic and budgetary battles. Also, as the game is judged by any one of them, there is no such thing as a friendly intelligence agency. The bias runs this way: I give them something, I've lost something. Law enforcement agencies have a similar mindset.

In a recent article, John Deutch, a former director of central intelligence and Jeffrey H. Smith, a former CIA general counsel, summarized the problem: "Historical boundaries between organizations remain, stymieing the collection of timely intelligence and warnings of terrorist activity. This fragmented approach to intelligence gathering makes it quite possible that information collected by one U.S. government agency before an overt act of terrorism will not be shared and synthesized in time to avert it."⁴⁷

The dead weight of America's intelligence bureaucracy clearly choked off movement of vital information in the weeks leading up to the events of September 11. Still, the anxiety imparted by September 11 was widely shared, and U.S. allies have since then been freely offering useful intelligence, although they began complaining after a

time about a one-way flow of information, of getting nothing back from Washington.

The intelligence agencies of Central and Southwest Asia tell their American counterparts what they want them to hear. Last January, President Bush and senior U.S. officials, referring to documents acquired in Afghanistan, amplified warnings about possible terrorist attacks. But intelligence officials were unable to identify actual plans for another attack. "That's where you need to get multiple sources and interview folks," one official said. "So far, we haven't had enough to issue any new alerts."⁴⁸

Briefly, a pivotal question is whether governments, starting with America's, can develop the habit of insisting that intelligence services work together closely on an uninterrupted basis and give up narrowly focused, bureaucratized behavior patterns. The question has nothing to do with technological gaps between various services or other differences and everything to do with the give-and-take of politics, bureaucratic and international.

Bush's people must soon decide whether the primary goal in the war on terror is subduing terrorist groups, starting with al-Qaeda, that threaten the United States, or pressuring, if not removing, regimes of which the administration disapproves. A useful admonition was provided by Vincent M. Cannistraro, formerly chief of counterterrorism at the Central Intelligence Agency and director of intelligence programs for the National Security Council in the Reagan administration: "Some Defense Department officials argue for broadening the anti-terror war by confronting Hezbollah, Hamas, Palestinian Islamic Jihad and others.... The Justice Department seems determined to take its own anti-terror war into the jungles of Colombia. But such moves risk inviting new enemies to kill Americans even before we have completed our mission to stop al Qaeda operations.... We need to be aware that by confronting terrorists who do not have a 'global reach,' we will do little to

deter the next round of terrorism here in America and may even enhance the danger."⁴⁹

The term "failed states" is in fashion. And a survey of those among them that may harbor threats of the kind we have to think about offers a view of the world that is nearly panoramic. They cannot all be helped or stabilized. The task will be to select a few states that have special regional significance and, if helped, could begin to diminish tensions and moderate behavior within their neighborhoods. This huge task could only be taken on by a special group of countries—perhaps the membership of the G-8, with a chair for China if it chooses to take part. The group would have to work closely with the United Nations and other organizations, global and regional. What all this requires, notably of Washington, is a style of political leadership that eschews unilateralism and anchors itself to a multilateral approach to national security.

It should be clear that terrorism is not a single problem, but an element of a larger problem. Thus far, however, Washington's concern with the causes of terrorism has been minimal. Its actual focus appears to be regime change—establishing an impression at home of threats emanating from the "axis of evil" states, plus a few others. The focus of all or most of the U.S. effort and investment is on dealing with terrorist acts and potential acts. The numbers in the 2003 budget say as much. U.S. foreign aid to promote democracy, address poverty, and improve education will increase by \$226 million, or one-fourth of the \$1 billion that President Bush said the United States now spends *each month* on the war in Afghanistan. And only \$66 million of the aid money is actually new, the rest having been shifted from other State Department accounts.⁵⁰

Other members of the coalition, starting with Britain, take a very different view. Last December, Sir Michael Boyce, chief of Britain's defense staff, warned publicly that

"we have to attack the causes, not the symptoms, of terrorism.... Our experience in Malaya and Northern Ireland teaches us that concentrating on the hearts and minds side of the campaign enables us to gain information, to isolate the terrorist and strike him. This is an approach that has proved successful in counter terrorist campaigns the world over.... The desire to use greater forces with less proportionality...will end by radicalizing the opinion of the Islamic world in favor of Al Qaeda."⁵¹

The Tasks Ahead

Neutralizing al-Qaeda and moderating the Arab-Israel conflict are the twin first-priority tasks confronting the Bush administration. Helping to stabilize Afghanistan is another.

The need to do something about Iraq's weapons of mass destruction is apparent but less pressing and should not blur Washington's immediate focus. The problem of Iraq has little, if anything, to do with terrorism; and what to do about Saddam Hussein's weapons program is far from clear. Equally unclear is just what he has in the WMD bag and whether he could effectively deliver what there is. There is no shortage of opinion on this subject, much of it shrill. Hawkish elements favor combining a surgical but massive assault from the air against Saddam's military infrastructure with a (hoped-for) insurrection abetted by U.S. special forces. Invading Iraq with a force of appropriate size and preceding the step with a bombing campaign would be a more realistic option. However, in the time required to prepare militarily for such a step, not to mention building political support for it, Saddam could be under heavy pressure, especially from countries that matter to him, to meet his obligations to the United Nations. Specifically, he could and should be pushed to allow random inspections of his weapons facilities wherever located. That has been the stated objective of the Bush administration, as it should be. Ridding the

region of Saddam, however desirable, is far less important than eliminating his weapons programs. His refusal to allow inspections on a scale sufficient to pinpoint the location of these programs, along with their scope, would justify changing Iraq's regime by force.

Political support for the military campaign that may be required could be difficult to secure. Russia, various European allies, and countries within the region would want to know whether Washington was ready to accept heavy casualties. More to the point, they would be likely to withhold support unless convinced that the U.S. campaign would succeed in ridding the scene of Saddam and his Baathist regime, and that a generally acceptable successor regime could be installed. Imparting credibility to this latter assurance would be difficult, since a successor to Saddam that various key parties can live with has yet to be identified, and improvisation is not likely to meet the test.

Since the Second World War, the Arab world has been largely shaped by transient passions, notably anticolonialism, nationalism, socialism, and Islamism. The single constant, apart from corrupt and/or incompetent regimes, has been the Arab-Israeli conflict and a perception throughout the region that Washington shares responsibility with Israel for the plight of the Palestinian people. The effects of the dynamic aroused by all this will damage American interests, along with everyone else's, including Israel's.

The Middle East and Persian Gulf constitute a region linked both by geography and persistent instability, of which the Palestine problem is one of two immediate sources. The other lies in the difficulties posed by Iraq and Iran and the uncertainties arising from Washington's controversial policy of dual containment and its application. A key variable is Bush's evolving relationship with Putin and what sort of grand bargain they can work out on a range of issues. Russia has priority interests in Iran, Iraq, Afghanistan and, of course, the Central

Asian republics. This is the region in which terrorism and organized crime intersect. The United States clearly needs close Russian support in coping with these persistent threats to security. In getting this support, not least from Russian intelligence, Washington will have to meet Moscow at least part way.

Conclusions

European capitals, probably including Moscow, are unsure about which threats are seen by the Bush administration as most immediate and worrisome. They don't know whether Washington's first priority is isolating, if not removing, regimes of which it disapproves or thwarting al-Qaeda. George Tenet, the director of central intelligence, estimates that only 20 to 30 percent of the cells deployed by the al-Qaeda network in some 50 countries have been destroyed.

The gap between Washington and allied European capitals is widening. It is partly about soft power versus hard power. Politically, Europe is somewhere between unable and unwilling to invest a lot in creating hard power—a capacity to wage high-intensity conflict. However, the United States still regards the first and best answer to threats to security as lying in preponderant military force. European governments, without exception, see military force as a complementary tool in the campaign against terrorism—less essential than a soft-power mix of intelligence, law enforcement, border and financial controls.

A growing chorus of critics within and beyond the region deplore the thrust of U.S. policy and objects to what it sees as pronounced unilateralism and indifference to the interests of others. In describing Iraq, Iran, and North Korea as an "axis of evil," President Bush was taking a line that was—is—radically different from that of close U.S. allies, including Britain.

The question arises: can a strictly me-first policy accommodate itself to the requirements of the era in which we find

ourselves? Those in Washington who echo Palmerston—states don't have friends, they have interests—may not understand that advancing one's interests is normally a process of give and take, even if the only superpower doesn't have to give as much as others. At some point, the Bush people may recognize their need for partners, as distinct from disgruntled yea-sayers. Such is the hope. ●

Notes

1. U.S. Department of State, *Patterns of Global Terrorism 2000*, April 2001, p. iii.
2. U.S. Department of State, "Principal Themes on Missile Defense," memorandum, 2001, p. 1.
3. David von Drehle, "Terror Taken Up a Notch," *Washington Post*, May 13, 2002.
4. Matthew L. Wald, "Electric Power System Is Called Vulnerable, and Vigilance Is Sought," *New York Times*, February 28, 2002.
5. Joseph Cirincione, "A Much Less Explosive Trend," *Washington Post*, March 10, 2002.
6. "Foreign Missile Developments and the Ballistic Missile Threat through 2015," unclassified summary of a National Intelligence Estimate, December 2001.
7. "A Report of the Department of Energy's Non-Proliferation Programs with Russia," Russia Task Force, Howard Baker, Lloyd Cutler, Co-Chairs, January 10, 2001, pp. vi–vii.
8. *Ibid.*, pp. iii–iv.
9. Bruce Blair, "Nuclear Dealerting: A Solution to Proliferation Problems," *Defense Monitor*, vol. 29 (April 2000), p. 4.
10. Sam Nunn. "When Bush Meets Putin," *Washington Post*, June 12, 2001.
11. "Remarks of Senator Carl Levin on National Missile Defense," National Defense University Forum Breakfast on Ballistic Missile Defense, May 11, 2001.
12. Joseph Cirincione, "The Ballistic Missile Threat," Carnegie Endowment for International Peace, Washington, D.C., June 18, 2001.
13. Geoffrey E. Forden "World War III? Now?" *New York Times*, September 6, 2000.
14. Geoffrey Forden, Pavel Podvig, and Theodore A. Postal, "False Alarm, Nuclear Danger," *IEEE Spectrum*, vol. 37 (March 2000), pp. 2, 8.
15. Bruce Blair, "Empty Reassurances," paper prepared for the Congressional Program's U.S.-Russia Relations Conference, August 21–25, 2000.
16. See John Steinbruner, "The Significance of Joint Missile Surveillance," Committee on International Security Studies, American Academy of Arts and Sciences, July 2002.
17. *Ibid.*
18. Interview with Mike Shuster, National Public Radio broadcast, November 7, 2001.
19. Steven Mufson, "The U.S. Worries About Pakistan's Nuclear Arms," *Washington Post*, November 4, 2001.
20. Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, cited in *Study on Asymmetric Warfare & Terrorism*, "Radiological Weapons as Means of Attack," Center for Strategic and International Studies, Washington, D.C., February 16, 2001, p. 114.
21. Matthew L. Wald, "Agency Weighs Buying Drug to Protect Against Radiation-Induced Ailments," *New York Times*, November 29, 2001.
22. Spencer S. Hsu, "U.S. Doles Out Bioterrorism Funds," *Washington Post*, February 1, 2002.
23. Dibya Sarkar, "The Weakest Link," *Federal Computer Week*, February 8, 2002.
24. Gwen Robinson and Adrian Michaels, "US Signs Deal on Smallpox Vaccine Supply," *Financial Times*, November 29, 2001.
25. *Inside the Pentagon*, newsletter, November 29, 2001, p. 1.
26. Justin Gillis, "FDA Releases Anthrax Vaccine to Military, Approves More," *Washington Post*, February 1, 2002.
27. Eric Pianin, "Study Assesses Risk of Attack on Chemical Plant," *Washington Post*, March 12, 2002.
28. Richard A. Falkenrath, "Confronting Nuclear, Biological and Chemical Terrorism" *Survival*, vol. 40 (autumn 1998), pp. 43–65.
29. Michael Donovan, "The Mass Casualty Threat of Biological and Chemical Warfare Agents," unpublished research paper for the Center for

- Defense Information, Washington, D.C., November 20, 2001, pp. 5–6.
30. Jessica Stern, "Apocalypse Never, But the Threat is Real," *Survival*, vol. 40 (winter 1998–99), p. 178.
31. Donovan, "Mass Casualty Threat of Biological and Chemical Warfare Agents," p. 6.
32. Dennis M. Gormley, *Dealing With the Threat of Cruise Missiles*, Adelphi Paper 339 (London: International Institute for Strategic Studies, June 2001), p. 7.
33. David Tanks, "Assessing the Cruise Missile Puzzle: How Great a Defense Challenge?" Institute for Foreign Policy Analysis, Washington, D.C., October 2000, p. 7.
34. Letter from Undersecretary of Defense Paul Kaminski to Congressman Floyd D. Spence, cited in Tanks, "Assessing the Cruise Missile Challenge," p. 8.
35. "The Missile Technology Regime," Arms Control Association Fact Sheet, (www.armscontrol.org/factsheets/mtrc.asp), p. 1.
36. Carnegie Endowment for International Peace, "The Missile Technology Control Regime: How Effective Is It?" *Non-Proliferation Project*, vol. 4, no. 7 (Washington, D.C., April 12, 2001), p. 2.
37. Tanks, "Assessing the Cruise Missile Puzzle," p. 10.
38. *Ibid.*, pp. 26, 40.
39. Vivek Raghuvanshi, "Secret India-Russia Pact Produces Cruise Missile," *Defense News*, June 18–24, p. 3.
40. Gormley, "Dealing with the Threat of Cruise Missiles," pp. 18–19.
41. Thomas Wilson, Testimony before the Senate Intelligence Committee, February 2, 2000.
42. "Ballistic and Cruise Missile Threat," National Air Intelligence Center, Wright-Patterson AF Base, Ohio, September 2000, p. 23.
43. Cirincione, "The Ballistic Missile Threat," p. 1.
44. Elaine Sciolino and Steven Lee Myers, "U.S. Study Reopens Division Over Nuclear Missile Threat," *New York Times*, July 5, 2000.
45. Interview with Brent Scowcroft, "Frontline," Public Broadcasting Service, November 14, 2001.
46. William J. Broad, "Surge of New Technologies Erodes U.S. Edge in Spying," *New York Times*, September 20, 2001.
47. John Deutch and Jeffrey H. Simon, "Smarter Intelligence," *Foreign Policy*, January/February 2002, p. 64.
48. David Johnston and James Risen, "Seized Afghan Files Show Intent, Not Plans," *New York Times*, February 1, 2002.
49. Vincent M. Cannistraro, "The War on Terror Enters Phase 2," *New York Times*, May 2, 2002, p. 27.
50. Robin Wright, "Don't Just Fund the War, Shell Out for Peace," *Washington Post*, March 10, 2002.
51. Sir Michael Boyce, "UK Strategic Choice Following SDR & the 11th September," speech, Royal United Services Institute, December 13, 2001, p. 3.

Mr. SHAYS. Dr. Krepinevich, you have a lot of pressure on you because you really have three colleagues who preceded you who have outstanding statements. But I am comfortably able to tell you that I am sure you will do well, because I took your statement home last night, and I thought it was a wonderful summary of the issue. But we do need to get you the mic, don't we?

Dr. KREPINEVICH. Thank you, Mr. Chairman. Like my colleagues, I will summarize my remarks.

Mr. SHAYS. Like most of your colleagues.

Dr. KREPINEVICH. First, let me applaud the subcommittee, for tackling this issue. It really is the missing link. Strategy is about connecting ends and means. We know the ends we want to achieve: the defeat of international terrorism. And we know the means that we are going to apply, in the terms of the budget and the resources and the capabilities that we are putting to the task. What we need to worry about is that although the means are impressive, we only get to spend them once. If we choose the wrong strategy—or if we choose the right strategy, but do not have sufficient resources to implement it—what we end up doing is not only wasting resources, but also wasting time, neither of which can be recovered. With that in mind, I would like to offer some comments on the administration's set of strategies.

I do not believe that there is anything inherently wrong with having a hierarchy of strategies as long as they are comprehensive, consistent, and, of course, as long as the strategy is effective. What I think is somewhat remarkable is that we actually have public statements about strategy in wartime. For example, after Pearl Harbor I don't recall President Roosevelt saying, it's Germany first, which was our grand strategy, going after Germany before Japan. I don't remember anyone saying that General MacArthur would be pursuing an island-hopping strategy, avoiding Japanese strong points, as his approach to solving the problem of defeating Japan in the Pacific. Football coaches don't advance or announce their game plans in advance, nor do chess masters before a chess match. So I do think that—and I would assume, and, quite frankly, I would hope that there are some key aspects of our strategy for waging war on terrorism that are not public, that are classified, to include some of the capabilities and forces that support this strategy.

On the other hand, we have to find some way of squaring the circle, because Congress is responsible for the power of the purse, they are responsible for the war powers of this country. And so Congress must identify a way to assess the administration's strategy. I have no solution for this dilemma.

With respect to the strategies themselves, I think there is much to applaud in terms of the effort on the part of the Bush administration. We need to recognize that this is not just a variation of former strategies. In fact, what we are dealing with here is a dramatically different kind of threat or combination of threats: the prospect of rogue states developing weapons of mass destruction and perhaps having to these weapons fall into the hands of terrorist organizations. Certainly this is about as big a shift in the kind of threat environment as we have seen since the early days of the cold war.

Second, I think this set of strategies is clearly an effort to provide at least some point-of-departure strategic guidance both in general terms and in terms of the key specific areas that may define the competition, such as cyberspace, the issue of financial laundering and so on.

If that is the glass half full, I think we also need to examine the glass that's half empty. If you look at historical experience, we only have a few data points. We did not really come up with a strategy for dealing with the Soviet Union, a comprehensive strategy, arguably until 1950, when you had NSC-68.

We also found that we had to constantly evolve the strategy to reflect changing circumstances. As you pointed out, Mr. Chairman, we had in 1953 the Solarium group meeting, when President Eisenhower took office, to revise and revisit the strategy that had been laid down several years earlier. So, again, this is not a situation where you come up with a strategy overnight. It is not a fast-food approach to strategy. This is going to require a lot of work, a lot of hard, intellectual work to address a lot of the questions, quite frankly, raised by you and by my colleagues here today.

I would point out also that both NSC-68 and the Solarium group were classified undertakings.

The strategies that I reviewed, to the extent that I could, given that at least one of them was classified and, as our colleagues pointed out, there were several of them just released recently, do lead to some unanswered questions. This gets back to my point that further work is going to be needed. I will just raise a few here for your consideration.

One, as Mr. O'Hanlon said, is this issue of preemptive attack. If we really do decide to pursue this policy, or this strategic pillar, against terrorists or rogue states, we are going to have to get a lot better at things like surprise, stealthy deployments, operating along short time lines, and operating over long distances. I don't think you can conduct a surprise attack with a precursor being months' long negotiations with allies as to whether or not you can use their forward bases. So, initiatives by the Defense Department such as converting Trident submarines to provide for the stealthy insertion of Special Operations forces or the increase in the size of Special Operations forces, would be consistent with that kind of strategy.

Of course, we are also modernizing our Air Force to deploy large numbers of short-range aircraft to forward bases which may not be available, at the same time developing no new long-range air capability.

So, again, I think at some point you have to begin to look at the strategy and the means and see where the links and the disconnects are and, again, to paraphrase from my colleagues, to see if the dots all connect correctly.

In terms of port security, I think the issue was raised by Michael O'Hanlon. Where is the emphasis? Is it at the port of origin where the goods coming to our shores originate? There has been talk in the Pentagon about a maritime NORAD, about a naval force that will intercept suspicious cargo ships the way our missile defenses are meant to intercept incoming warheads. Or is it at the port of entry? Or is it a combination of these things? If so, which has pri-

ority? And over what time will we phase in these various elements of our strategy? What is the standard of performance? How many cargos are we supposed to be able to intercept and check out?

So, in the area of port security, it seems to me that we know there is a danger there. We know there is a threat. We are devoting means to address it but not quite clear what the linkage is between the means and ensuring that we achieve our ends.

If you have a strategy that recognizes that deterrence doesn't work against terrorists and you may not be able to intercept every terrorist attack, than a big part of your strategy has got to be damage limitation, or what we call consequence management. How do you limit the damage of a successful attack? Because that can go a long way toward defeating terrorism. Where is the responsibility? With the Federal Government? With State governments? With local governments?

For example, once an attack occurs in an American city, is it that city's responsibility alone to deal with it? I would suspect that we would want to mobilize resources and flow them toward that city. Well, who controls those resources? Can the Federal Government put the arm on other cities' resources now at its disposal to go to the city that's been attacked? Have we built in the transportation assets that allow us to rapidly reinforce the city that's just been subjected to attack? Is it that way across the board?

Or do we recognize that, for example, in the case of first responders, those people who are on the scene first, you are not going to be able to reinforce them. Either they are going to be able to do the job quickly, or it's going to get out of hand. Have we really thought through the process, the linking of ends and means, to make sure that we have an effective defense in dealing with consequence management?

There are other matters that deserve consideration. The role of our allies. Our alliances were formed in a different era, when there was much more common agreement about what the principle threat to our security was. We find ourselves needing allies more in the global war on terrorism but perhaps in some cases being able to rely on them less. Certainly we want to rely on them for different things.

There's a new division of labor. We don't want tank armies so much as we want good intelligence, for example. So how do we devise a new division of labor, and what does that say about our strategy? What resources can we free up to accord to other priorities?

I will just speak very quickly on cost-imposing strategies. It's kind of an arcane term, but it's a strategic term. Bottom line: they spend \$1 million, we spend \$100 billion. That's an awfully effective strategy. Part of our strategy, part of our strategic development, has got to answer how are we going to off set their ability to pursue cost-imposing strategies on the United States.

In summary, I would say that the administration's efforts represent an important initial effort to address the most dramatic shift in our threat environment since the early days of the cold war. The effort is both impressive and, I would argue, incomplete. We are only at the beginning of a major process, primarily intellectual, to come to grips with this threat and make sure that we have

a strategy that can effectively apply our limited resources to achieve the very worthy ends that we seek.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman.

[The prepared statement of Dr. Krepinevich follows:]

Combating Terrorism A Proliferation of Strategies

Testimony Presented to

The House Committee on Government
Reform

Subcommittee on National Security,
Emerging Threats, and International
Relations

Andrew F. Krepinevich

Center for Strategic and Budgetary Assessments

March 3, 2003

Introduction

Mr. Chairman, it is an honor to appear before you today. The Subcommittee has identified an important issue that merits serious consideration and debate. Strategy, at its core, is about linking ends and means. An optimum strategy identifies the limited resources, or means, at hand and provides the methods that enable them to be applied efficiently to achieve the ends desired. In the case of the Global War on Terrorism, the end sought by the United States is to reduce the terrorist threat to the point where “Americans and other civilized people around the world can lead their lives free of fear from terrorist attacks.”¹ The country must put the lives of some Americans in harm’s way achieve this end, and devote a substantial amount of its national treasure. These resources, although quite impressive, are finite. Moreover, they can only be spent once. If we choose the wrong strategy, or execute the right strategy ineffectively, we will have wasted both time and resources, neither of which can be recovered.

As the Subcommittee has noted, the Bush Administration has set forth a number of strategies for addressing the Global War on Terrorism. This raises several concerns. One is whether the strategies are logically consistent. Another is whether they, in fact, constitute a coherent strategy for achieving the end—victory in the war on terrorism—that we desire.

A thorough evaluation of these issues with respect to the various strategies cited by the Subcommittee would take considerable time and effort. Unfortunately, some important elements—such as the Bush Administration’s budget and *The National Strategy for Combating Terrorism*—have only recently been released. *The National Military Strategic Plan for the War on Terrorism* is a classified document, and thus is not available for public inspection.

There is nothing inherently wrong with having a hierarchy of documents that provide a statement of our strategy at various levels of detail. In fact, this is what the Bush Administration seems to have done. The issues here are consistency and comprehension. One would expect, for example, the *National Security Strategy of the United States of America* (hereafter referred to as the *National Security Strategy*) to serve as a capstone document. Both the *National Homeland Security Strategy* (which, as its name indicates, addresses domestic aspects of the Global War on Terrorism) and the *National Strategy for Combating Terrorism* (which addresses the overseas aspects of the strategy) can focus more specifically on their part of the strategic mission, so long as they are consistent with the *National Security Strategy*, and identify how they are integrated, one with the other.

At a more detailed level, certain specific aspects of the larger strategy—those dealing with denying terrorists with access to weapons of mass destruction (i.e., *The National Strategy to Combat Weapons of Mass Destruction*), defend against cyber attacks (i.e., *The National Strategy to Secure Cyberspace*), and restrict terrorist access to financial

¹ National Strategy for Combating Terrorism, February 2003, p.1, <http://www.whitehouse.gov/news/releases/2002/12/WMDStrategy.pdf>

resources (i.e., *The National Money Laundering Strategy*)—can provide comprehensive guidance on how the strategy is to be implemented. Again, the question of having a set of strategies is not one of propriety; rather, it concerns consistency with the broader strategic guidance and integration with the other associated elements of the strategy.²

Another matter to keep in mind in evaluating these strategies is that the practice of publicly proclaiming strategies for defeating one's enemies has clear limits. Public strategic statements are useful in focusing the attention and efforts of the nation. It can also reassure allies, and perhaps deter adversaries. However, there are limits to how much we want our enemies to know concerning how we plan to defeat them. Just as a football coach seeks to keep his game plan from the opposing coaching staff, and a chess master refuses to elaborate to his opponent on his strategy for the coming match, some details of our strategy for defeating terrorism should remain secret. This, of course, presents a dilemma for Congress, which must discharge its responsibility for providing the means to execute the strategy. However, Congress appropriates billions of dollars each year to so-called Black, or classified, defense programs. Thus it would seem that methods can be found that enable Congress to make informed judgments on the kind and scale of resources required to execute a strategy for the Global War on Terrorism.

I would now like to turn to the matter of the strategies themselves. Do they form a cohesive framework? Are they comprehensive? Have they eliminated gaps and duplications in programs? How will we know when the strategy is effective? Before providing some observations on these issues, it is worth examining the threat addressed in the strategies advanced by the administration.

The Nature of the Terrorist Threat

Following the attacks against New York and Washington on September 11, 2001, the United States finds itself engaged in its first war of the 21st century. This war against international terrorist aggression—ancient in its origins, but new in its form and intensity—presents a very different set of challenges, and requires a wholly different response from the more traditional conflicts that have dominated America's recent history.

The United States now confronts radical Islamic terrorist organizations practicing "asymmetric warfare"—aligning their strengths against America's weaknesses, rather

² For example, to the extent that disrupting money laundering is considered an important part of the strategy to deny terrorists access to weapons of mass destruction, both *The National Strategy to Combat Weapons of Mass Destruction* and *The National Money Laundering Strategy* should not only be consistent with the higher-order strategic documents (e.g., *The National Security Strategy*; *The National Strategy for Combating Terrorism*), but also with one another. Moreover, each strategy should explain the role it plays in the other's efforts; i.e., how the strategy for dealing with money laundering helps to address the challenge weapons of mass destruction, and how the strategy for denying terrorists access to WMD supports the strategy for denying terrorists money laundering (for example, as a means of organizing and transferring to enable WMD development, or for buying WMD).

than attacking the US military head-on, tank against tank, fighter against fighter.³ This enemy sees America's long borders and open society as vulnerabilities that enable infiltration and attack coordination. Respect for the right of privacy and freedom from unreasonable search and seizure, and the diversity of America's nationalities and faiths, are seen not as democracy's legacy, but rather as shields behind which to plan the next attack. The information revolution that has fueled much of the world's recent economic growth is exploited by this enemy to coordinate its attacks.

Radical Islamic terrorist movements in general and al Qaeda specifically seek to:

- Remove western influence (more specifically, US influence) from Islamic states. This would include US military influence (e.g., military bases; combined training exercises) and cultural influence; and
- Overthrow those regimes in Islamic states that do not follow the path of radical Islam, so as to establish radical Islamic regimes under their domination.

For their part, radical Islamic terrorist organizations have pursued a strategy of the weak, similar to those pursued by others engaged in insurgency warfare.⁴ Realizing they are no match for the United States when it comes to conventional forms of military power, they have opted to pursue a cost-imposing strategy by threatening the United States itself, as well as US forces and facilities in the Middle East region.⁵

³ To be sure, radical Islamic terrorist movements are not the only terrorist organizations that have the potential to threaten the US homeland and America's vital interests abroad. However, as measured by level of military effort and funding, they are the *de facto* focus of the administration's Global War on Terrorism, and for good reason. Radical Islamic terrorist organizations have been, by far, the principal source of terrorist activity directed against the United States over the last two decades.

⁴ Indeed, it is more profitable to consider the threat posed by terrorist organizations like al Qaeda as an insurgency movement—albeit one that operates on a global scale and may have access to destructive capabilities far beyond those traditionally associated with insurgent movements. Just as insurgent movements seek to advance from acts of terrorism to guerrilla warfare involving larger forces, so too did US forces encounter al Qaeda military formations during Operation Enduring Freedom in Afghanistan. While the attacks on the United States can be viewed from a number of perspectives, one intriguing possibility is that Osama bin Laden intended for the attacks, by their success, to trigger an uprising in the so-called Arab Street that would depose certain weak Islamic regimes in favor of al Qaeda-friendly governments. This recalls the Tet Offensive by the North Vietnamese during the Vietnam War, in which the Communists attempted to trigger a collapse of support for the pro-US regime in Saigon. In both instances, the attackers were proven wrong about the level and depth of popular commitment to their cause.

⁵ A cost-imposing strategy is one in which one of the competitors is forced to incur greatly disproportionate costs in order to offset a threat posed by its rival. For example, during the Cold War the US bomber force enabled the United States to pursue a cost-imposing strategy against the Soviet Union in that it cost Moscow far more to develop, field and operate its national air defense system than it did for the US Air Force to develop, field and maintain its bomber force. Similarly, the terrorist attacks of 9-11, which cost perhaps \$1 million to mount, finds the United States spending tens of billions of dollars to prevent similar terrorist attacks.

In recent years, Islamic terrorists have moved to escalate the conflict both horizontally and vertically.⁶ Horizontal escalation occurred when they expanded their attacks to the United States. The terrorists' willingness to target noncombatants has complicated the US defense problem even further, and also increased the cost of establishing effective defenses. The terrorists' strategy appears based on the premise that the United States will prove unwilling to bear these costs over the long term, producing a dramatic reduction or even withdrawal of US influence from the Middle East, paving the way for the victorious radical Islamic forces and rogue states to topple any local regime that opposes them. Hence the focus on cost-imposing strategies and challenging America's willingness to persist over the long haul.

The vertical escalation in the terrorists' campaign involves ratcheting up the level of violence to effect greater death and destruction. Their willingness—indeed, determination—to kill large numbers of noncombatants indiscriminately and their desire to use or acquire weapons of mass destruction is a critical characteristic of this conflict: the concentration of far greater destructive potential in the hands of small groups than has heretofore been the case.⁷ This "Democratization of Destruction" may be facilitated not only by terrorist efforts to develop chemical, biological, and radiological weapons themselves, but also to acquire them through various sources. Of particular concern are the so-called Axis of Evil states.

The radical Islamic terrorist strategy has produced some positive results, particularly when contrasted with the conventional wars involving Islamic forces. Conventional conflicts such as the June 1967 Six-Day War and the 1991 Gulf War yielded Arab military disasters of historic proportions. By contrast, Hezbollah succeeded in coercing the US component of the Multilateral Force out of Lebanon in 1984 following the attack of a suicide truck bomber on the Marine Corps barracks in Beirut, killing 241 marines.⁸ Israel has found coping with terrorism difficult. Arguably, the Intifada campaigns contributed significantly to Israel's withdrawal from southern Lebanon and to Palestinian efforts to extract concessions from the Israeli government. In summary, radical Islamic terrorists have pursued a cost-imposing strategy within a protracted conflict which has produced what success the cause of Islamic fundamentalism has seen to date in its efforts to eliminate US influence and weaken, if not destroy, Israel.

⁶ Horizontal escalation refers to shifting the geographic focus of the conflict. The attacks of 9-11 marked a shift from attacking US facilities, citizens and forces overseas, to attacking the US homeland itself. Vertical escalation refers to increasing the intensity of the conflict. The strikes against the World Trade Center (in particular) and the Pentagon were intended to kill tens of thousands, far in excess of the casualties suffered in attacks such as those on Khobar Towers, the US embassies in Kenya and Tanzania, or the USS Cole. The 1993 terrorist attempt on the World Trade Center is a notable exception to this pattern.

⁷ Aum Shinrikyo, a Japanese terrorist organization, attempted to develop both chemical and biological agents, and to use them to create mass casualties. The United States was subjected to a number of terrorist anthrax attacks of unknown origin in the weeks following 9-11. During Operation Enduring Freedom evidence emerged of al Qaeda's attempts to obtain WMD, to include radiological weapons (e.g., "dirty bombs").

⁸ The Multilateral Force comprised units of the American, British, French and Italian armed forces.

These are remarkably ambitious objectives for a terrorist organization. For many years, terrorists were a nuisance dealt with by a state's law enforcement capabilities. Why have they become such a problem now? The reason is that they may be gaining access to far more formidable means of destruction—to include weapons of mass destruction—than were available to terrorist groups only a few years ago. This effort may be aided and abetted by rogue and enabler states, which provide terrorists with sanctuary of one sort or another. It is a cruel irony that, as 9-11 shows, in addition to the havens provided by tyrannical regimes,⁹ terrorists have also found sanctuary in democratic states. Countries such as Germany and America, where laws designed to protect a citizen's right of privacy and freedom of movement, were exploited to facilitate acts of terror.

A particular concern for the future is that rogue states, once they have acquired weapons of mass destruction, may through design or laxity allow terrorists access to them. In short, the terrorist threat to the United States cannot be viewed in isolation from those states that enable them. This includes states and institutions that, by accident or design, enable the financial flows that support terrorist organizations.

Of course, to the extent radical Islamic terrorist movements are successful, we may expect to see others imitate their strategy. The threat of terrorist attack on the US homeland may be adopted by other terrorist groups, or even states that covertly sponsor such groups for the purpose of conducting ambiguous aggression against the United States. Consequently, the United States must develop a comprehensive strategy for dealing with the terrorist threat, one that addresses not only terrorist organizations themselves, but their sponsors—witting and unwitting. As radical Islamic terrorist movements manifest many of the characteristics of an insurgency, any US strategy must address how the root causes that animated these movements in the first instance can be eliminated while preserving American principles and interests.

Strategic Shift: From Cold War to Hot Peace

During the first decade of the Cold War the United States debated a range of options for addressing the threat posed by the Soviet Union, which aggressively (and successfully) sought to develop nuclear weapons. Among the options considered were preventive war and preemptive attack. Preventive war was ruled out, primarily owing to the risks involved. The Eisenhower Administration's defense posture of Massive Retaliation saw military leaders planning for "Massive Preemption" in the event preparations for an imminent Soviet first-strike nuclear attack could be detected.¹⁰ As the Soviet nuclear

⁹ For example, Syria (along with Iran) supports Hezbollah, the Islamic terrorist group operating out of Lebanon. The group is responsible for the suicide bombing attack on the US Marine barracks in Beirut in 1983 and of a series of kidnappings and murders of US officials. Iraq plotted the assassination of former President Bush during his visit to Kuwait in 1993, provided sanctuary to terrorists such as Abu Nidal, provides support to terrorist organizations such as Ansar al Islam, and offers subsidies to the families of Palestinian suicide terrorist bombers to encourage such attacks on Israel.

¹⁰ McGeorge Bundy, *Danger and Survival* (New York: Random House, 1988), p. 321; and Marc Trachtenberg, "A 'Wasting Asset': American Strategy and the Shifting Nuclear Balance, 1949-1954," *International Security*, Winter 1988/89, pp. 44-45. See also Marc Trachtenberg, *A Constructed Peace: The*

arsenal grew, notions of preventive war or preemptive attack faded from senior policy debates. Eventually Washington settled on a strategy of containing communism, as represented by the Soviet bloc. This strategy was pursued through a military posture of deterrence and flexible (often interpreted as proportional) response in the event deterrence failed.

Washington continued to follow this strategy in the first decade following the Soviet Union's demise. Rogue states like Iran, Iraq, and North Korea were to be contained and deterred from committing aggression. The United States imposed economic and political sanctions against them roughly similar to those imposed on the Soviet Union.

The strategy has produced mixed results. No rogue state successfully engaged in aggression. However, terrorist organizations, and radical Islamic terrorist groups in particular, have not been deterred from executing a series of attacks on US forces and facilities abroad, to include the Khobar Towers attack in 1996, the bombing of US embassies in Africa in 1998 and the attack on the USS Cole in Yemen in 2000. An attempt to blow up the World Trade Center in 1993 was foiled. A second attempt, using hijacked airliners in September 2001, resulted in the destruction of both World Trade Center towers and coincided with a similar attack that damaged a major portion of the Pentagon. This was followed by a string of anthrax attacks, origins unknown, focused primarily on targets in the New York and Washington areas. Recent attacks include those against a French oil tanker off the coast of Yemen, against tourists in Bali and Kenya, and on an airliner in Kenya. Israel continues to be subjected to suicide terrorist attacks.

Whereas deterrence and containment worked well during the Cold War, the same cannot be said of their effectiveness against radical Islamic terrorist movements. Moreover, while terrorist attacks have not produced prompt results, they have proven to be a more effective challenge to US and allied interests than traditional forms of aggression, and are proving increasingly destructive. It is no small irony that deterrence worked far better against a superpower rival during the Cold War than it has against radical Islamic terrorist organizations, which are microscopically weak when compared to the Soviet Union. Islamic terrorist groups, who have no country to defend, and no industry or national infrastructure to lose, have proven poor targets for retaliation, as a series of US retaliatory strikes over the last two decades has demonstrated.¹¹

Making of the European Settlement, 1945-1963 (Princeton, NJ: Princeton University Press, 1999), pp. 162, 164.

¹¹ US military operations in response to terrorist acts include the aborted Desert One hostage rescue mission in April 1980, naval bombardment and air strikes over Syria in December 1983, air strikes against Libya in 1986, cruise missile attacks against Iraq following the assassination plot against former President Bush in 1993, and cruise missile attacks against suspected terrorist facilities in Afghanistan and Sudan in August 1998 following attacks on US embassies in Africa. No retaliatory strikes were conducted by the Clinton Administration for the terrorist attacks on US forces at Khobar Towers or against the USS Cole. One also recalls an attempt at what might be termed appeasement by the Reagan Administration in offering arms to the Islamic Republic of Iran in exchange for the release of US hostages being held by Islamic terrorist organizations with strong ties to Teheran.

Until recently, it might have been argued that even if deterrence had failed against such groups, the damage sustained would be relatively minor. In the wake of 9-11, that argument is more difficult to make. Moreover, the Bush Administration argues that Iranian and Iraqi state efforts to develop weapons of mass destruction, combined with their association or sponsorship of terrorist organizations, means the risk of terrorists obtaining access to WMD for their use is significant and growing. Should terrorists gain access to advanced biotoxins or nuclear weapons, their ability to wreak destruction would increase dramatically. Given the United States' failure to dissuade countries like Iran and Iraq from pursuing WMD, and its failure to deter terrorist attacks against its interests overseas and its homeland, the Bush Administration now finds itself seeking other remedies in the wake of deterrence's failure.

In the global war on terrorism—against al Qaeda, specifically—the United States has accepted that relying on deterrence, and its threat of retaliation, to prevent future attacks, is a dead end strategy. In its place, Washington has embraced preemption—destroying al Qaeda elements wherever they can be found, before they can undertake yet another strike.¹² At the same time, Washington also declared that states sponsoring terrorist organizations with global reach (e.g., al Qaeda) would also be liable to attack.

The administration's strategy accepts the fact that the United States is already at war with al Qaeda and likely other terrorist groups, and thus must pursue a war-winning strategy. The administration also realizes that it must also address the danger posed by those states who offer sanctuary and support to such terrorist organizations, either consciously or unwittingly. Finally, the administration recognizes that it must not only deal with the symptoms of the terrorist movements—armed terrorist attackers—but the root causes—political, economic and social—that spawned terrorism in the first place

A Proliferation of Strategies

The Bush Administration has responded aggressively to terrorist attacks of 9-11 and those that followed. Al Qaeda's principal base in Afghanistan was attacked and its terrorist forces scattered. Enormous resources are being devoted to wage war against al Qaeda and associated groups, and to better prepare for the longer-term terrorist threat. Major new organizations have been created to address the challenge. In the largest restructuring of the US Government since the 1947 National Security Act that established the organizational basis for the 40-year struggle with the Soviet Union, Congress established the Department of Homeland Security. A military structure—Northern Command—has been created to organize America's homeland defenses. These are impressive initiatives. They reflect both a determination to prosecute the war vigorously, and to devote a remarkable amount of resources to provide for America's security.

There is, however, another matter that must be addressed: a strategy that links the means with their purpose, which is to win the Global War on Terrorism. The Bush

¹² This may be an overstatement. After all, if the United States is already at war with al Qaeda, preemption in the traditional sense is not really what is occurring. Rather, the US military is attempting to defeat an enemy before he can marshal his forces for yet another attack.

Administration has developed what can be described as a series of strategies related to how to prosecute the war. The various strategies include the:

- *National Security Strategy of the United States of America*
- *National Homeland Security Strategy*
- *National Military Strategic Plan for the War on Terrorism*
- *National Strategy for Combating Terrorism*
- *National Strategy to Combat Weapons of Mass Destruction*
- *National Strategy to Secure Cyberspace*; and the
- *National Money Laundering Strategy*

Although at first blush this plethora of strategies appears daunting, there is nothing inherently wrong with having multiple strategies, or sub-strategies, as long as they are logically consistent. What is also important, of course, is that the strategies provide a comprehensive method for applying the means available—and those being requested—to the task at hand: winning the Global War on Terrorism.

Such a strategy must also elaborate on the roles and responsibilities of the relevant departments and agencies of the federal government, their relationship with state and local governments, and the linkages between the United States, its allies, and various nonstate actors (e.g., international institutions, corporate America).

Much to Applaud—Much to Be Done

The Bush Administration deserves credit for its efforts to tackle the multidimensional aspects of the Global War on Terrorism, both in terms of developing strategies that provide a blueprint for addressing the threat, in its efforts to restructure our organizations to deal with the threat, and in requesting resources that will enable these organizations to execute its strategy.

While the administration may deserve an “A for effort,” however, the fact remains that such the dramatic reorientation of the US national security strategy, to include the structure and resources for executing it, will not be easily accomplished. One only needs to recall the effort required in the late 1940s and early 1950s by the Truman and Eisenhower Administrations to come to grips with the threat posed by the Soviet Union, Communist China, and the development of nuclear weapons. While the Defense Department was created through the National Security Act of 1947, it took until 1958 before its structure was refined (and even then only partially) to address the new circumstances in which America found itself. And even though the Soviet threat was identified at the end of World War II, it took the United States five years, until 1950,

before the famous NSC-68 strategy of containment was developed to guide its efforts in the long-term competition. The bottom line is that we should be under no illusion that the administration's set of strategies is anything more than a start on the serious intellectual work that must be done to develop a refined strategy for what is almost certain to be a protracted conflict against transnational terrorist organizations with global reach.

Unanswered Questions

As noted earlier, given time and security constraints, I was unable to undertake a comprehensive review of the strategies prior to this hearing. However, based on a preliminary assessment, it is possible to raise some issues for consideration.

Preemptive Attack. The administration's strategy calls for preemptive attacks on terrorist organizations planning attacks on the United States. For example, intelligence may provide information on the whereabouts of terrorist leaders, or on the production of weapons of mass destruction. The former target is fleeting, while the latter target may require special targeting.¹³

This implies an ability to act quickly and strike without warning and over great distances. It may also require special capabilities or weapons. In such instances, where time is short and maintaining the element of surprise is key, the United States will not have the luxury of negotiating access to forward bases or moving forces into the region prior to executing its preemptive attack. The administration's move to increase the size of US Special Forces fits this strategy well. However, there also appear to be several disconnects. For example, Special Forces conducting preemptive strikes will likely need stealthy means for insertion and extraction. The Navy's conversion of Trident ballistic missile submarines to carry significant numbers of Special Forces may provide a partial solution. What is lacking is a commitment to stealthy means of aerial insertion and extraction. Similarly, the Air Force plans to purchase over 2,000 short-range tactical aircraft, which will require access to forward bases for their operation. Yet the Service has no plans to produce any long-range bombers over the next several decades.

Border Security. The strategies do not provide guidance in any great detail as to how America intends to maintain control over its borders against the infiltration of terrorists or weapons—weapons of mass destruction in particular. Take the issue of ports. There are a number of possible options for providing port security. One is to place the burden on securing cargo containers on the port of origin. The United States might certify certain overseas ports as meeting certain US-established security standards. Container ships carrying such certified cargo containers might have their offloading process expedited (think of the E-Z Pass toll lanes on highways). Those that arrive from uncertified ports would be subjected to rigorous inspections.

¹³ Of course, it is possible that these threats might be identified in a country that is allied to the United States in the Global War on Terrorism. If so, that country, perhaps with US assistance, could deal with the danger.

Another alternative would be for US intelligence services to monitor cargo shipped from ports in hostile or unstable states. Suspicious cargo ships could be monitored by a “Maritime NORAD” which might intercept and search ships on the high seas, much as the North Korean ship carrying ballistic missiles was searched recently near the Persian Gulf. Yet another alternative would be to place most of the responsibility for port security on local governments at the US point of entry. Or, over the longer term, it may be possible to use mobile offshore ports, based on oil platform technology, as a means of safely screening incoming cargo at sea before it proceeds to coastal ports.

There are yet other options, and combinations of options are possible, too. In short, a good strategy would set forth how port security is to be achieved.

Damage Limitation. A key part of the administration’s strategy is to limit the damage arising from a terrorist attack on the United States. This ability is a function of the scale of effort (e.g., the size of the organizations—first responders, decontamination elements, the National Guard, etc.—involved in consequence management), their level of training (i.e., their effectiveness) and how quickly they can be brought to bear on the area attacked. One strategic option for addressing this challenge is to place responsibility primarily with state or even local governments, to include the funding and physical assets. Another option would be to place responsibility primarily with the federal government, to include funding and physical assets. The former offers the advantage of assets optimized for local conditions. The latter offers the advantage of being able to mobilize far larger forces much more quickly to limit the damage of an attack.

An example may serve to make the point. Assume there are 100 cities in the United States at risk of terrorist attack. The former option would allocate resources on a per capita basis to each municipality to be employed as it best sees fit. The latter option would find the federal government emphasizing the placement of resources in the highest risk cities, and also in those cities that could serve as regional transportation hubs for rapid reinforcement of damage limitation forces at other cities.

In short, the federal government would allocate resources on a threat basis, not a per capita basis. Moreover, it would position these resources in a manner that would enable the government to rapidly dispatch damage limitation forces to any city that had been subjected to attack. The latter option, or strategy, assumes that terrorists cannot mount attacks in all 100 cities simultaneously. It thus provides an initial defense capability for each city (i.e., first responders) while relying on its ability to mobilize and deploy quickly external forces to enhance the city’s defense, should it be attacked.

The strategic option chosen has major consequences. If the former is chosen, it will be much more difficult to achieve a high level of damage limitation than in the latter case, where resources can more easily be mobilized and committed. If the latter case is chosen, greater emphasis will have to be given on the means for rapid transport (i.e., airlift). The latter option also assumes federal responsibility for a significant part of the training of such organizations.

There are still other issues that should be addressed in the process of refining the administration's strategies for combating terrorism.

The Role of Allies. We are truly in an era of ad hoc coalitions. We need allies for the war on terrorism, but we will need them for different kinds of support than in the past. Areas such as human intelligence, special operations, maritime interdiction and stability operations are likely to take on greater prominence. The extent to which we fashion coalitions and identify a division of labor among these mission areas can help inform the mix of capabilities the United States must maintain or develop to implement its strategy.

Strategic Phases. It is difficult to discern whether the administration's strategies are to be pursued in phases, or simultaneously. This is important as the effectiveness of execution may depend on certain things being accomplished before others are initiated (e.g., establishing US port security mechanisms while other options—such as port of departure controls or the use of offshore ports—are being developed).

Competitive Strategies. The administration's strategies discuss US strengths in the Global War on Terrorism and how they might be exploited. Competitive strategies takes this concept one step further and asks how America's enduring competitive advantages might be aligned to exploit terrorist enduring weaknesses to the United States' advantage within the context of a long-term competition. This strategic concept, which was developed to deal with the enduring Soviet threat during the Cold War, may have important applications in this new protracted conflict. Far less is mentioned in the strategies concerns how the terrorists might pursue their own competitive strategies. A good strategy not only takes into account what might be done to exploit US advantages, but also what can be done to mitigate US weaknesses.

Cost-Imposing Strategies. The attacks on 9-11 not only brought the war on terrorism home to the American people, it also represents a cost-imposing strategy for terrorists. A cost-imposing strategy is one in which one of the competitors is forced to incur greatly disproportionate costs in order to offset a threat posed by its rival. The terrorist attacks of 9-11, which cost perhaps \$1 million to mount, led to the United States spending tens of billions of dollars attempting to erect defenses against terrorist attacks. At least one of the administration's strategies should address where the United States is vulnerable to cost-imposing strategies, and how this vulnerability might be mitigated or offset. This is particularly important in protracted conflicts, where the costs borne must also be endured over a long period. Similarly, the strategy should address options for pursuing cost-imposing strategies against terrorists. The matter of cost-imposing strategies is one area that is particularly suitable for security classification.

Planting the Garden. To the extent that radical Islamic terrorism represents an insurgent movement, dealing with it requires more than denying these groups sanctuaries from which to mount attacks on the United States. It also involves attacking the root causes that spawned the terrorist movement in the first instance. These causes are typically political, economic or social in nature. Because the problems are deep-rooted, they are not often quickly ameliorated. This is another reason why the Global War on Terrorism is

almost certain to be protracted in nature. The Bush Administration's strategies discuss the issue, but only in passing. There is little meat on the bones of this important element of the strategy. A strong case can be made that a strategy for stability operations is just as important as, say, a strategy for dealing with illegal financial flows.

Conclusion

My tentative conclusions, based on a limited, preliminary assessment of the administration's strategies are that:

- They represent an important initial effort to come to grips with perhaps the most dramatic shift in the threat environment encountered by the United States since the dawn of the Cold War.
- While in many instances the effort is impressive; it also is incomplete. *This may also be because significant portions of the strategy are classified—and rightly so.* Thus, given historical experience, these strategies should be viewed as initial steps on the road to developing a comprehensive strategy for the long-term Global War on Terrorism.
- Consequently, a major intellectual effort should be undertaken toward this end.

Mr. SHAYS. I really appreciate all four of your testimonies. I am so eager to jump in, but I am going to call on Mr. Janklow to start.

I would just make a comment that will tell you where I'm coming from. At this table, we had an individual who was a doctor of a major medical magazine; and he said, before—he said, I want to put something on the record. And this is what he basically put on the record. He said, my greatest fear is that a small group of dedicated scientists within a country can create an altered biological agent that could wipe out humanity as we know it. That to me was a very real statement of why we can't wait for a lazy country to step in and stop a small group of scientists from creating a biological agent that could wipe out humanity as we know it.

In other words, it's not just those countries that seek to work with terrorists but those who tolerate them. And there is not a chance in heck that I would think that we would wait.

Which gets to a topic that you had brought up, Dr. O'Hanlon, and all of you did, and that's the whole issue of preemption. My view was that what we would have over the course of the next few months and maybe years is, with the world communities, how do we define when preemption has to happen?

So I took an advantage that I don't often do as chairman to just jump in here, but, Mr. Janklow, you have the floor for 10 minutes.

Mr. JANKLOW. Thank you, Mr. Chairman; and thank all four of you gentlemen for your testimonies.

Dr. O'Hanlon, you were specific with respect to certain areas. When we look at the structure of America, I will call it the infrastructure of this country, given the way history's developed or we have developed, but for the military bases, the banks, the jails and prisons, nothing has been built secure. Everything, 100 percent of our country is open. Closing those doors and getting into a public safety mentality is just an incredible cultural and physical shift for us. What do you think is the threat assessment with respect to our public utilities, specifically the electrical grids? All we have are fences that say high voltage, keep out, where we have the transformers. Yet disabling a transformer is probably one of the easiest things in the world to do.

There isn't a backlog of transformers in this country on the shelf. In the event someone were to start to bring the electrical system down, you could make whole areas of this country uninhabitable for months. Were it to be done in the wintertime, it is incalculable how we could deal with it and maintain our standard of living or not turn on each other. Have you ever had a chance to assess the question with respect to the electrical utilities or the natural gas utilities where every so many miles they come up out of the ground, with the pumps and the monitoring, and it would be a no brainer just to throw a log chain around them and drive off, pulling them apart. Do you have any comments, sir?

Dr. O'HANLON. Those are very tough questions, Congressman. I share your understanding and your concern on electricity in particular because it's so hard to fix. My understanding—and I'm not an expert in this area—but it could take several months to repair some of the kind of damage one might imagine.

Mr. JANKLOW. That's correct.

Dr. O'HANLON. During that period of time, as you say, the economy and even the basic ability to ensure heat and other needs for people would be really at risk.

I think the way you have to prioritize homeland security, because, as you pointed out, we don't want to protect every restaurant and every movie theater in this country, at least I hope we don't have to get to that point, but you have to prioritize. And I think the way you do is to say major loss of life, major economic damage, or major damage to the institutions of this country such as government. Those are the sorts of things we have to focus on most intently. If there is a plausible risk in one of those areas, you should think hard about doing something about it if you can.

As Andy Krepinevich says, there may be situations where the cost is just too high. But I think you have identified a couple of areas where the cost is not that high, and it's a matter of scrutinizing our vulnerability, and I think you've identified a couple of important ones that I should have added to my list.

Altogether, by the way, I think we can make very good progress on about a \$50 billion a year Federal budget for homeland security. So, we're moving in the right direction, but we're not there yet.

Mr. JANKLOW. Thank you.

Mr. Newhouse, I gathered from your testimony you're rather critical of the way things are going under the current administration; and I notice from your resume that you were a senior policy advisor to Strobe Talbott with respect to Europe. But I was wondering, did he take your advice on how to deal with Europe during the time you were an advisor to him?

Mr. NEWHOUSE. You can say, yes, sometimes, but rarely. Because I found myself in persistent low-intensity conflicts with the State Department bureaucracy. As I'm sure you know, when you go up against the organized bureaucracy, the cards are weighted against you. But it was fun. I wasn't there very long. I was there for the last 3 years of the Clinton era.

Mr. JANKLOW. And, sir, if I could ask you with respect to—a lot of your testimony dealt with our relationship vis-a-vis Israel, our policy, the policy enunciations by the President. Do you know of any strategy that any President has ever employed with respect to Israel that worked, or the Middle East, Israel vis-a-vis its relationship with the Palestinians, given the uniqueness of the threat to Israel, the constant?

I mean, I just—I was there last week—2 weeks ago on an International Relations Middle East Subcommittee trip; and it was amazing, just amazing that, to go into grocery stores, you go through magnetometers. You go into malls, you have the wand put over you. You can't go into public parking. The cost of the society for public protection, none of it contributing to economic growth, is an unbelievable drag. And that country is so small you could put six of them inside my State. I just—I can't even imagine a United States with that kind of drag.

My question is, do you know of any administration that's had an effective policy with respect to the peace aspects of that area?

Mr. NEWHOUSE. Well, I would say there were two. First, the second Eisenhower administration. After the Suez crisis began—and

I no longer remember what became of that effort. Maybe it was the political calendar. I don't remember.

But I think the most striking example of this was the Presidency of George W. Bush after the Gulf war, starting with the Madrid Conference. What transpired during the Madrid Conference when he had all the key players around the table led eventually to the Oslo Peace Process. I think the Oslo Peace Process set in motion other agreements, and they kind of sustained what appeared to be a sustained process which ended abruptly in 1995 with the assassination of Prime Minister Rabin.

I would submit that the time between the collapse of the Soviet Union and September 11th was a kind of parenthesis during which the one event of lasting historic importance would have been the assassination of Rabin, because that ushered in instantly a Likkud government, and things began to go from bad to worse.

Now it's not as if the blame falls largely on Israel. I mean, it also falls with great weight on the Palestinian Liberation Organization and its leadership. But I think the Palestinian moderates by and large understand what's been happening to them, and they—and since it has been happening to them in the most injurious and painful way, they would like to change things, including changing the leadership. They can't change their leadership so long as you have got this nexus of political heavyweights starting with the Likkud party and government that lashes out at the PLO leadership and quarantines it, makes a hostage of its leader, says that you have to change this.

Mr. JANKLOW. Sir, if I can ask you, let's just assume that in this country we were dealing with an element, a group of people, where the leader funds—contributes funds toward those that are blowing up our people and our facilities, where they contribute support, public rhetoric to give aid and comfort to those that are trying to drive us out of the area. I'm not being overly sympathetic to the Israeli position as much as I am to say, put yourself into their mentality and then deal with what Yasir Arafat and his group have done with respect to the safety in the area or the neglect. It's not benign neglect, it's far more than the benign, and one can understand the activity that individuals take as self-preservation.

You know, I visited the American military when—Patriot missile units that were in Israel a week ago, and I frankly was dumbfounded at the attitude that all of those soldiers had, the men and women had, all the way down to the lowest enlisted ranks as to what their mission was and how important they felt they were for the security and stability in that particular area.

I am just wondering if you have any insight, sir, as to—coming back to homeland security. What is it that we can do in this country to make it safer? I mean, obviously, September 11th, we found out how vulnerable we were. To the extent anybody's committed and was willing to commit suicide, you can wreck a powerful lot of damage over and over and over. What it is that we are not doing that we ought to be doing specifically?

If you could list the things, Mr. Newhouse.

Mr. NEWHOUSE. Well, I began my statement by suggesting what I thought we should do first and foremost in bringing stability or

greater stability to the region—and I mean the entire region. That is to restart the Middle East Peace Process.

Mr. JANKLOW. No. No. I mean the United States, here.

Mr. NEWHOUSE. Yeah. But only we can do that. Nobody else can restart the Middle East Peace Process.

Mr. JANKLOW. So you are suggesting—

Mr. NEWHOUSE. The Europeans can't do it. The quartet, that is to say, the combination of the United Nations, the European Union, Russia, they cannot do that without the other member of the quartet, the United States, taking the lead. It is just wholly unrealistic.

Mr. JANKLOW. So what you are suggesting, sir, is to the extent that the Middle Eastern Peace Process gets started or gets on a better track, things will be safer in the United States?

Mr. NEWHOUSE. Yes, indeed. Because I think that not only does the region use the Arab—the Palestinian-Israeli issue as the principle—one of the principle tools for generating recruitment in the region, but I think that the larger part, most of the Islamic world is profoundly sympathetic to the Palestinian cause.

Mr. JANKLOW. Would that explain the explosions then, for example, in Bali, in Indonesia?

Mr. NEWHOUSE. I don't know, sir. Partially. Because—I mean, I think these things are really all connected. What is it that inspires an organization like al Qaeda? It's more than one thing. I mean, I think the leadership probably wants to divide Islam from the Western world if it can. But it uses whatever grievances, tools, that it has available to it; and this is certainly a big one.

Mr. JANKLOW. Thank you.

Mr. NEWHOUSE. Sir, can I just make one—with response to one of your other questions, when you said that these people are being terrorized and being killed, I'd just make two comments. The number of people being killed over—since the Second Intifada began, there's been a great disproportion, a tragic number of Israeli citizens have been killed, that's true. But a considerably larger number of Palestinians have been killed in the process and a great number of Israelis, if they were sitting here, Israelis whom I know personally, would strongly agree with what I've said here. But they feel frustrated because they have very little control.

Amos Elon, one of the great Israeli writers, wrote recently: Israel's military power increases on a daily basis, and its security diminishes on a daily basis, because Israel is a small state with a low birth rate that lives in a huge sea of Arabs.

Mr. TURNER [presiding]. Thank you, Mr. Newhouse.

Mr. Gilmore, would you like to comment on some of the questions?

Mr. GILMORE. Mr. Chairman, respectfully, it is a policy decision about whether the foreign policy of this country is going to shift with respect to support of Israel or their policies. That is not really the topic that we are discussing here today. We are discussing here today the question of what actions the Congress can focus on in order to try to make the homeland more secure. I think that was the essence of Congressman Janklow's ideas about this.

I'm concerned, frankly, about some of the things that I'm hearing here today. I think there is a risk here that we are being led down

the path of trying to address all vulnerabilities in the Nation. You cannot address all vulnerabilities of the Nation. Again, that was also said from the dais a few moments ago.

This Nation is a free country. It carries within, therefore, inherent vulnerabilities. But vulnerability is not threat. Threat is different. Threat is the things that the enemy has the capability of attacking, and they don't have the capability of attacking everything. They don't—the motivation to attack things and what things are vulnerable, and that is the threat, and that we can address. We can address that. If we tried to address everything that anyone could imagine, any terrorist could imagine, we are driving ourselves into being a financially exhausted martial state, which is exactly what the enemy probably would like to see us get to.

Instead, we have to address that, and then I think you go to a little different question, which is, how are we doing it?

We are setting up a major bureaucracy with the Department of Homeland Security, but what are we doing it for? That is the point to keep the eye on the ball about here. We don't want to get so tangled up in the administrative efforts to get it all to coordinate and work together we lose track of what we're trying to do, which is to address the potential threats of this country in a reasonable and prioritized way and to address what we really think the potential threats are.

And for what purpose are we doing that? I don't think it's to make ourselves a martial state. I think at some point it's to return to some sense of normalcy in this country, not a country like was being described someplace where we are constantly watched and constantly going through security measures at the grocery store and things like that, but to get back to the point where we protect ourselves to the greatest extent possible from reasonable, foreseeable risks and threats and then get on with our lives as free people. Otherwise, the enemy's won.

Mr. TURNER. Thank you, Governor.

Now, Mr. Bell, you will have 10 minutes.

Mr. BELL. Governor, I couldn't agree with you more when you suggest that there is no way possible for us to do everything to keep the homeland safe. I have said for a long time that you could take every security precaution known to man, some even unknown at this particular point in time, and still have someone willing to kill themselves in order to kill other people. That you're not—there are going to be instances where you can't defend against that.

I do believe, though, that after September 11th we live in a new world in some negative ways but also some rather positive ways, one being that there has been an awakening and there is a sense of alertness in America that has never been seen before. Things that not too long ago would have probably been taken for granted, an unattended piece of luggage in a crowded facility, will now be pointed out to a security guard. I daresay if an individual like Timothy McVeigh went and tried to purchase an inordinate amount of race car fuel that would be reported to some authority. If someone signed up for a flight class and expressed no interest in taking off or landing the aircraft, that type of suspicious behavior would be reported.

What I am curious about is that the only way that works and that sense of alertness leads to greater security is if there really is communication between the various law enforcement authorities; and I hope that is something positive which has come out of September 11th, too, because we have all heard the stories of turf wars between various law enforcement entities, the breakdown in communication, information not being transmitted to where it should be going. I'm curious as to what your feelings are on that particular subject, whether we really have seen better communication between the different levels of law enforcement.

Mr. GILMORE. Congressman, of course, it has to be addressed on two levels, one is technological and the other is cultural.

The technological part is the part we still have to reach for, the ability to have some interoperability to address the spectrum issues, to get local responders some capacity to have the ability to use their intercommunications, even to allow some spectrum to allow people in the private sector to be able to have some communication capacities within themselves; and that remains I think ahead of the Congress. But that's the easier part.

But that's the easier part. The more difficult part is the cultural problem and that is getting intelligence organizations to communicate with each other. This is an issue we first began to address in the year 2000 with our report to the Congress on December 15, 2000, where we pointed out that there was not information passing back and forth laterally among Federal intelligence organizations—FBI, NSA, CIA, all the rest of them. And more importantly, there was not information traveling vertically up and down the line between Federal, State and local people.

We pointed out that while within the Federal system, clearances are granted routinely to elected officials in the Congress, there are no clearances granted routinely to people in the State bureaucracy who actually have the primary responsibility to deal with these issues. I was the Governor of one of the two States directly attacked on September 11th, New York and Virginia were the two States directly attacked, and based upon that, I know from personal experience that there was difficulty with that.

In this past report, our fourth annual report, we recommended that there be a fusion center of intelligence information that would also have a role to play with Federal, State and local people all within the fusion center, the communication back and forth between Federal organizations as well. And a form of that was adopted by the President in his State of the Union address, and we are optimistic that will be structured in a way that it can be made to work.

There is a major issue of how you are going to conduct counterterrorism activity in the United States to gain that information to go into the fusion center from within the homeland. That remains controversial even on our commission, but we think that progress is in fact being made. I was briefed at the White House recently by Admiral Abbott, the acting Homeland Security adviser to the President, who has pointed out that there are efforts being made to create those channels up and down the line between Federal, State and local people.

Last point, condition orange has been widely criticized when it came to pass, but it does have some value, value in communicating with the terrorists, value in communicating with the American people so that there is not a shock if there's another attack, which would cause a stampede, an overreaction, which I think we are all concerned about; but also that condition also triggers automatic communications between Federal, State and local people which I thought was maybe the most significant point.

Mr. BELL. Dr. O'Hanlon, Chairman Shays pointed out that he liked you when he realized that you had served in the Peace Corps. I liked you when you started making my case for me on port security, and I greatly appreciate that. And when I was home a couple of weeks ago, I started talking to people about this, basically to raise the flag and see who might salute it.

But I am curious where we go from here, because it is a very legitimate point that when you look at the number of petrochemical plants we have located along the Houston ship channel and realize the vulnerability of those plants, and I hope the point you are trying to make is, right now, you can look at that and say, well, that is your problem or that's their problem. But if there is any kind of strike against that type of plant, then as you point out, it becomes our problem. So, given that, I am curious as to what you would recommend.

And one thing that I've considered—haven't actually proposed it yet, because I want to get input from other people such as yourself—but should we be looking toward some type of subsidy program for those types of facilities, to provide a certain amount of Federal assistance, because I do agree with you there, there is a line and there is an economic line that they will reach.

I think most of the plants in my district have taken extraordinary measures. There's one chemical plant that I visited that I thought I was going to have an MRI conducted before I gained admittance. They go through extraordinary precautions, but there are limits. And before they are going to go to the full extent, I think they're going to be looking to the Federal Government for some kind of assistance; and I am curious as to what your feelings on that would be.

Dr. O'HANLON. Thank you, Congressman.

Also wrestling with the point that Governor Gilmore made about how we don't want to get so caught up in homeland security that we bankrupt the country, it's a tough balancing act to work out. In our Brookings study, we came to a couple of conclusions. One of them is at the Federal level, we do need some more capability in institutions like the Coast Guard and in some of the port security funding to develop port security plans that, right now, I think Federal money needs to go up. It doesn't necessarily need to go up astronomically. The Coast Guard budget already is increasing, but I think the Coast Guard's fleet needs to get bigger. That's one piece of it, but it's not really your primary concern.

Your primary concern is actual site defense at the place we're talking about. And there, I think—personally, I am not strongly opposed to the idea of subsidies, but I am more intrigued, just based on my research and discussions with economists at Brookings, by an idea they came up within the course of our study, which is, re-

quire a certain minimal level of regulation, minimal level of security legislatively, but leave the primary effort to the private sector; require many of these facilities to have terrorism insurance, and then the insurance market will work to give people incentives to adopt best practices because they can offer lower rates to people who are adopting better security practices.

So that's a partial answer. It still doesn't get to your real concern of how do we make sure that these facilities aren't themselves bankrupted because we are asking them to adopt a more secure workplace. If the level of Federal regulation or State regulation is relatively modest, and we say, you have to do certain basic things, have monitoring of all your major entrances, have a certain number of security guards on duty, have a certain number of tests per year of your response capability, and then leave it the private-sector insurance markets to help give these people incentives to develop best practices, that may work better than either Federal subsidies. Because there are so many facilities to subsidize, I don't know how you draw the line or simply trusting the private sector to get it right on its own.

One more point, if I could bring in a separate example and I am sorry to go on, but skyscrapers, I worry about anthrax being introduced into the air intake of skyscrapers. As far as I know, there is still no Federal requirement or State requirement in most places that these air intake systems be elevated above street level or otherwise protected.

We don't want to fortify every building in the country and we don't want to mandate this happen immediately, because it would cost too much. But I think for large buildings, there needs to be a certain push by the Federal Government for these buildings to get more secure on how they handle their air circulation systems. And then, again, the insurance markets can give them incentives to do even more, and they can choose for themselves whether they can afford the additional measures like filtering systems in their air, circulation devices and that sort of thing.

I am not yet prepared to endorse subsidies because of the sheer number of facilities and the sheer cost of doing so, but I haven't ruled it out either, and maybe there are certain places we have to at least keep it in mind if the economies of these plants and facilities—if their budgets are so stressed by additional security they simply can't do it on their own, we may have to at least give them a temporary helping hand.

Mr. TURNER. Governor Gilmore, I appreciate your comment concerning the sharing of information between local, State and Federal Governments. I served as mayor for the city of Dayton, and we actually were one of the few cities and communities that actually held weapons of mass destruction exercises prior to September 11th. Attorney General John Ashcroft attended those exercises, and it was phenomenally helpful to our community when September 11th occurred, because we knew who was in charge of what; what streets were to be closed. We didn't run to the phone book to figure out what agencies we needed to coordinate with; there had already been an effort to put together coordination with the FBI, the sheriff and the like.

Recently, I attended a presentation by NCR concerning the application of business data collection software to homeland security issues, and one of the things that they discussed is that the business process of handling data and information technologies starts with the question "what information do we need to know in working backward in designing your systems."

So the question I have for you, Governor and Dr. O'Hanlon, is, in this process of making certain that we are sharing information, what should we be doing or how is it going—in our efforts to define what we need to be doing, what information is it that we need to make certain that we avail ourselves of as we look to sharing that?

Mr. GILMORE. I think that's a new topic. The issue of what type of data, I suppose you're really referring to, if you're talking about a National Cash Register-type of presentation, CR-type of presentation—

Mr. TURNER. It was interesting in the discussion because they talked about, do you start looking at what data you have and start sharing that, or do you start with the question of what do we need to know and what levels do we need to know it. And they clearly indicated, even from the business process, and they believe from the government and homeland security process, that there should be a process of defining what are those things that we believe that we need to know as we go through setting up our systems and sharing that information.

Mr. GILMORE. There has certainly been a lot of discussion going on about the DARPA program that the Pentagon was attempting to conduct, the total information awareness. It was depicted at its inception as being so broad that it just scared the living daylights out of everybody. And I think this Congress decided to put the clamps on that somewhat. So that was, I think, maybe a starting effort to determine what you need to know, and it may have been defined so broadly that it wasn't going to go anywhere.

So it may be that if we can go through a definition process, we can preserve civil liberties and the privacy and anonymity of people as Americans at the same time we are providing for the capability of our counterterrorism people to focus on the right kinds of individuals or people. But that's a definitional process that still has to be gone through.

I think it has to be handled with the greatest care, and the reason is that today we live in an America that has two elements. I am not sure it is unique, but yeah, it might be. One is the American media to fix and manage our problems. If we say we have this problem here and this great managerial class called United States of America 2003 is going to try to find some technological or managerial approach to fixing the problem, that would go to the question of how you define that.

And the second, that is probably unique in the history of mankind, is this enormous technological society we live in and the capacity to gather data and to hold data and to keep data, which does threaten the potential privacy and character of the values of the American people.

Do you have to strike that balance? I think it is entirely a policy question. You will be led, Congressman, to the sense that it is a technological question and a managerial question. It is not; it is a

policy question of how much you are going to permit to be accumulated in order to preserve the security of the country. That is a judgment call based upon the values you bring with you to the Congress.

Dr. O'HANLON. Congressman, in this dichotomy you put forth, do you take what information you have and process it more or do you go out and look for more? You have to do both, but I want to emphasize the second piece. I want to do the equivalent of Phoenix memos as much as we can.

So what I mean by that, I would like to see local, State and Federal law enforcement authorities sharing information. If we happen to see 10 places in the country where there are people casing airfields on the same day or two, you want to know that it's not just one isolated place, and if it happens in one place in South Dakota and one place in Virginia and one place in Maryland, no one ever knows that it's happened at all these places simultaneously.

What you want to do is piece that information together or have it in some kind of a data base where somebody with a creative idea can write a computer program and say, am I seeing any suspicious behavior that is systematic?

So you want to have data entered into your National Law Enforcement Information System that allows that kind of correlation analysis to be done. And whether it is medical supplies being stolen, airfields being cased, crop dusters being rented, there are a lot of things that can fall into the category of flight training—that we know very well from 2001—that you would want to know about, especially if they were happening at more than one place at a time, suggesting some kind of a conspiracy. And that's where you need to generate the data and probably more of the data than we have today, get it into the data bases and then allow some kind of central analysis through Homeland Security's Threat Analysis System.

That is the sort of thing I want to see much more of. And that is going to require cultural improvements and technological improvements, as Governor Gilmore said before. I think the Federal Government is going to have to ultimately support improvement in information technology at the State and local level much more and maybe even subsidize some of it.

Mr. TURNER. Mr. Newhouse, your comments were very interesting. Some of the analysis, I was concerned, certainly was so one-sided that it left out elements of what we all know is occurring.

You state that one of the issues that needs to occur is starting with an end to Israel's occupation of the West Bank. I didn't notice in your comments the call for the ending of suicide bombing attacks. Your statements appear to be solely placing responsibility on what we believe are the responsible states and democracies, instead of the parties that are doing very egregious acts; and I would like some of your comments about that.

Mr. NEWHOUSE. They certainly are egregious and self-injurious. They are also, if you like, a response to what they see as the illegal occupation of their territory and the settlement activity, which everyone has said, including President Bush, has got to stop.

There are also acts being committed by, if you will, rejectionist groups who are also terrorist groups. And the leadership, Mr. Arafat's leadership, which—his is really an awful leadership. It is cor-

rupt and it doesn't advance the interest of the Palestinian people in any way, but because it is weak, inherently weak, it is unable to do anything about these acts. It has actually tried and failed.

These acts you speak of are being committed by the terrorist groups, and these are not terrorist groups that export, but they are devoted entirely to harming Israel. But there is very little from here that we can do about it, other than—in my opinion, except for doing what I suggested that we do, which is restart the Middle East peace process.

Mr. TURNER. I would take it that you would not indicate that you believe that the suicide bombings are advancing the cause of a Palestinian state or resulting in a greater likelihood of that occurring?

I mean, it sets back, obviously, the peace process. And when their occurrence is neglected, in your comments, as merely a responsibility of—or the setbacks are a result of Israel's reaction, I think it doesn't provide us with the information that we need to come to a conclusion as to what really the United States needs to be doing.

Mr. NEWHOUSE. Well, I would agree with you that the acts of terrorism committed against Israel are certainly from the point of view of Palestinian interests and are deeply counterproductive. As of now, there seems to be very little that anyone can do about that directly. The Palestinian leadership has been unable to do anything about it; the Israelis themselves are unable to do anything about it because retaliation simply invites more of the same.

So it is kind of a demonic process going on, and as I said, there is very little, if anything, that the United States can contribute directly to heading it off, stopping it. But I think, in a larger sense, generating some stability out there and getting the sides together in a peace process, I think, is really the only weapon available.

Mr. TURNER. In your comments, you also talked about your concern about the preemption doctrine having an impact of exacerbating the threats in the United States, and you ended a paragraph with "Terrorism may be contained if intelligence services and police agencies acquire the habit of cooperating closely and with each other and suppressing their competitive instincts and preference for acting alone."

When the intelligence services and police agencies are cooperating, what action would you think would result from that?

Mr. NEWHOUSE. Well, if they are cooperating, then I think we are in very good shape. The problem is getting intelligence agencies and police agencies to cooperate systematically.

Frequently, they will cooperate. Going back to 1984, the Los Angeles Olympics—this may have been a first, maybe it wasn't the first, but we do know at that time the CIA and the FBI worked together very closely. They were under a lot of pressure from the White House to do exactly that. Not only that, but they were cooperating with their counterpart agencies in other governments, so that in the days preceding the Los Angeles Olympics, the FBI was able to assure Members of this body at that time that nothing would happen. They categorically said, nothing will happen at the Los Angeles Olympics; we've got these groups so penetrated, we know what they're thinking about before they think or what they're going to do before they do.

Much was the same at other major events: Y2K was an example, or the Gulf war when we rolled up 30 different plots to commit terrorist acts. The problem is, when agencies, both within our country and in their dealings with other countries, ramp up, in a phrase, for—to make sure nothing happens at a given time, the tendency then is—after nothing has happened and the event is over, is to ramp down and go back to the so-called “stovepipe method” where information is gathered at one level, or low level, if you will, and it drifts upward to the top and then it stops there, it isn’t transferred.

Because knowledge is power, and an agency that has information that perhaps another agency doesn’t have and uses that information to advantage, sometimes in the budgetary process—anyway, it’s counterintuitive to cooperate.

Mr. TURNER. Thank you.

Chairman SHAYS.

Mr. SHAYS. Thank you very much, Mr. Chairman. I am very eager to get into this dialog. I love this panel, and I guess I am fascinated by the issue because we fought for 4 years about this.

You know, in the beginning, Governor Gilmore, it was almost theoretical because, you know, we just didn’t come to grips with it fully until September 11th, but this is what I want to first start out with.

After September 11th the eight National Strategies to Combat Terrorism—this is what I am hearing from this panel—that after September 11th, the eight National Strategies to Combat Terrorism are a good start, but there is more work to be done.

And then, Dr. Krepinevich, I look at your statement and you say, you know, the National Security Act of 1947, it took until 1958 before it was structured. The structure was refined, and then you put in parentheses “and even then it was only partial.” We looked for a number of years before we had a reorganization that fit into this, in a sense, the strategy.

Now, so—and you had Eisenhower in 1952. I mean, you had all these stages of trying to improve this response to what was then the Soviet Union.

So what I want to know is, do you think this is a good starting point, if you all agree, and that we need more—more work needs to be done. And these are the areas I sense you are saying: Interrogation among the strategies; intelligence strategy, big question mark because that was pointed out as not existing. Should there be an intelligence strategy, or is there one that we just don’t sense? Ensuring that our national—not Federal strategies; I think, Governor Gilmore, that was your point, interesting concept of national versus Federal. And the need for more clear measures of effectiveness.

So that’s where the work needs done. And would you agree and would you want to speak to it, and would you want to add a fifth or sixth?

Dr. KREPINEVICH. I think we are off to a good start; we’re better off than we were a couple of years ago. I’m not sure what to compare this to.

Are the strategies integrated? I think, as certain members of this panel have indicated—let me speak for myself. I think there are

certainly gaps that have raised a number of issues that we have not come to grips with.

Do we need an intelligence strategy? I think if we are going to do what Governor Gilmore suggests, which I think is probably a way to get around the cost-imposing strategy that the terrorists intentionally or unintentionally are pursuing, the way to do it is to get them, as opposed to trying to provide an airtight defense ourselves.

Doing that certainly is going to require expert intelligence. We have underinvested in human intelligence of the kind that is typically crucial to breaking down these organizations.

Mr. SHAYS. So would your point be that we need an intelligence strategy added to this list of strategies and then integrate it?

Dr. KREPINEVICH. Certainly you need a strategy for how you are going to employ your terrorist assets. It should fall out of your overall strategy. For example, if you are going to emphasize preemption, then I think the weight of your intelligence effort is going to be overseas. If you are going to emphasize a layered defense of the continental United States and Alaska and Hawaii, then more of your intelligence efforts may be at our borders and internal to the United States, which require a different kind of intelligence.

So I do think the kind of strategy you choose begins to inform how you are going to apply your intelligence assets and what kind of priorities you are going to place on them.

In terms of measures of effectiveness, I think we've only begun to scratch the surface on this. For example, I think the National Strategy for Combating Terrorism says, we'll know that we've won when Americans feel safe and secure and free of a terrorist threat. That's probably true, but it doesn't really give the person who has to execute a strategy much of a sense of what they need to do to try and achieve that end.

I would say two strategic measures of effectiveness that I would certainly consider are: one, what is an acceptable level of damage for the United States to incur? If it's impossible to provide airtight security over the United States, what's an acceptable level of damage and can we achieve it? What strategic alternative can give us the best prospect of essentially suffering an attack and having an acceptable level of damage?

The other is our freedom of action, because success is not only our ability to defend ourselves here at home, but it's our ability to protect our vital interests overseas. If we feel under such risk of attack here that we forgo our ability to, for example, protect critical areas whether it's East Asia, the Persian Gulf where we have vital interests, then we will have been deterred because of our vulnerability here at home or our ability to deal with the threat abroad.

So I do think that in terms of measures of effectiveness, again you can go up and down the line, whether it's dealing with cyber attacks—

Mr. SHAYS. Bottom line, there needs to be a lot more improvement and the whole issue of whether we're effective or not in determining how we'll even measure effectiveness?

Dr. KREPINEVICH. Absolutely.

Mr. SHAYS. Mr. Newhouse, do you want to speak to the issue of improving integration? Do we need an intelligence strategy, na-

tional versus the Federal issue and measures of effectiveness and any other strategy?

I am asking you, Mr. Newhouse. If you don't want to speak to it, I will go to Dr. O'Hanlon.

Mr. NEWHOUSE. Mr. Chairman, I think we spent a lot of time on this today, and I think Governor Gilmore and Dr. O'Hanlon would have a lot more that would be useful.

Mr. SHAYS. Let me get to you in another question.

Dr. O'Hanlon, one thing I say about a Peace Corps volunteer is, we were taught to understand the people that we lived with, and there were things that we did and said that when you understood their culture, you were able to interact and communicate with them.

Is there a role that needs to be played here in our strategy on terrorism as well? I am jumping ahead—do you know what I just asked you?

Dr. O'HANLON. It's a tough question. Clearly the answer is yes. You need to understand your partners and the needs of other countries. I don't know how to build it into a formalized process like this with today's focus on security strategies.

Maybe what I would say is that the National Security Strategy, which really should be at the pinnacle and does have some discussion of the needs of developing countries, to take one category of overseas partners, it sort of gets cheapened when there are all these other strategies that are out there. And I worry about the proliferation of documents, because we should all still be reading and developing and debating the National Security Strategy, and we did for awhile in the fall.

And then preemption was the flavor of the month for a few weeks, and now we're on to other documents. And there's a lot of stuff in the National Security Strategy that has nothing to do with preemption, as you well know, largely this economic assistance issue for developing countries who are very important partners of ours in counterterrorism.

So it's not a very clear issue.

Mr. SHAYS. I kind of got you off the topic here. I was eager to share a bias that I have here without thinking it through.

Let me ask you to address the issue—the eight strategies are a good start, better integration. Do we need an intelligence strategy—national, not Federal—and the whole issue of effectiveness. Comment on any of those?

Dr. O'HANLON. I will comment on a couple of them. I had the opportunity to at least tangentially talk about a couple of the others already.

The issue of national versus Federal response, it does occur to me that we need to spend more time thinking about the State and local role. Obviously, Governor Gilmore has more experience than I do. But I, for example, have some contacts at the L.A. city council who were very concerned about the delay in the first responder fund over the last year. And Washington let down the States and the local governments in having this stalemate on that.

And one can look for different people to blame, but the bottom line is, I think, Washington didn't get the job done until too late. We spent a whole year when we should have been dealing with

first responder capacity, improving that, and we really didn't do much.

In fact, I'm told that in L.A. city council debates, advocates of doing more were often stymied because others would say, Washington is going to help us pretty soon, we don't have to find the money, just wait and the \$3.5 billion is going to start to come our way. And people who wanted to find local funds had their own argument for finding local funds undercut by this promise from Washington that was not fulfilled for a full year.

So maybe—you know, I hate to call for more strategies, but maybe we do need to get the Federal versus national distinction a little more prominent in our thinking and spend more time—I was delighted to see the Governors put some pressure on Washington a couple of weeks ago, and I think we'll need more of that.

Mr. SHAYS. Governor Gilmore—and I will take my next round to talk about the whole issue of multi—unilateral, and this whole issue of preemptive.

Mr. GILMORE. Congressman, it is a good start. We didn't have a national strategy before September 11th, of any kind; now we have eight strategies. And I guess I would like to think about them a little bit and the Commission will think about them a little bit. I believe that will be a topic we will address in this 5th year for the Congress and for the President and try to think through that.

I think we should make sure they don't contradict each other or that they don't place different emphases. But I think we're going to find that these are—supplement each other. Some of the strategies like the cyber and so on like that are points of emphasis, and I am not sure that I see them as something where you have to try to conglomerate them into one overall strategy. I think it might work out all right, but we will look at that.

The intelligence piece is really tricky. This is very, very difficult. We have placed a great emphasis on this all of our 4 years that we have been in existence and recommended that stovepiping be broken through and fusion center be created and the culture of separation be broken down between all these different agencies.

The trick is that you do all that and you run the risk of contaminating the society by looking over the shoulder of regular people out there who are just trying to live their lives every day. This is tricky. It means that we all believe that you have to do effective sharing of information to get at the bad guys, but at the same time, you have to find some method to not be looking over the shoulder of the good guys.

This is a very tricky challenge—national, not Federal, absolutely. And I think that this is the real, maybe one of the focuses. I would say to you, Congressman Shays, that the danger here is, we are going to get so caught up with how you put the agencies together and the Department together, that you implement everything, that we lose some focus and momentum toward actually doing the things that are going to be necessary. I am uneasy with the idea that every witness who comes before you for the next year is going through a list of vulnerability that he sees within his own State and then, of course, naturally demand money to go into that State to take care of that vulnerability. That's not a very good approach.

Instead, you have to find an all-hazards type of approach, one that really focuses on enabling the States to create State-oriented plans in cooperation with their localities so that instead of worrying about any individual chemical plant, you enable your localities and your States to observe that plant, all the plants, all the railroads, all the airlines, and enable them to be watched in a reasonable way and to respond if an attack does occur and to circumscribe the potential attack.

The key issue is implementing that, really not worrying so much about the organization as implementation of the program to, in fact, get out here and to get proper funding in accordance with the proper strategy, in accordance with a proper State plan and make sure that they are properly equipped, enabled, and they know who is on first and that it's properly exercised and ultimately measured.

Mr. SHAYS. Mr. Chairman, I would love to come back. When the Governor has had a chance, I would love to get into the issue of preemption.

Mr. JANKLOW. Go ahead and then I'll go.

Mr. SHAYS. Dr. Krepinevich, do you agree with Dr. O'Hanlon that a policy of preemptive self-defense should be more implicit than explicit?

Dr. KREPINEVICH. I agree with him to the extent that, the option of preemption is nothing new. For example, in the Solarium Study you cited, one of the three groups explicitly looked at conducting what was called preventive war against China. President Kennedy also explored in great detail and actually engaged the Soviets in discussions about a preemptive attack on China's developing nuclear facilities.

Certainly, President Clinton debated with his security advisers the prospect of conducting a preemptive attack on the North Korean reactor at Yongbyon. So this is not new; it has always been an option in our strategic arsenal.

I think perhaps by stating it as boldly as the President did, it might have garnered some unwanted attention on the part of the administration.

On the other hand, I think it's also necessary to point out to people that the last big threat that we faced, the Soviet Union, was a threat that we felt could be deterred; and so we put a lot of our eggs in the basket of deterrence. And that is why we had public statements of strategy, because again we wanted to get into the minds of the Soviets. We wanted them to understand that any unacceptable action on their part would produce catastrophic consequences for them.

Well, what do you do when you can't deter a group that can inflict substantial damage on your country? You have to begin to reweigh your balance of options. And this administration has argued for preemption—which is really preventive war in the case of Iraq—and I'm not quite sure how you preempt somebody you're already at war with; we are already at war with terrorists—but at any rate, I think you've got to prepare the American people for the fact that we are going to be acting perhaps quite differently than we have in the past. And the reason is because our traditional reliance on deterrence has been eroded.

And you have to prepare the American public and you have to make the case to its elected Representatives for their support to develop the capabilities, because they are not identical to the kinds of capabilities you would want for a posture of deterrence.

Mr. SHAYS. Governor Gilmore, would you speak to this issue next? I would just preface it by saying, I think this is a huge issue that there has to be lots of debate about.

Dr. O'Hanlon, I don't come down on your side of the argument because it strikes me that the world community has to know that they can't allow a small group of dedicated scientists within their borders to do something that could wipe out humanity. We have to be honest with our own folks and say, this isn't—this needs to be stated explicitly, because this is the world you live in. It's a different world.

So I am giving you my answer to it, but I'd be happy to have you comment to it, Governor.

Mr. GILMORE. Congressman, I think we have an obligation to be very precise on our threat assessment before we decide to take serious military action. The intelligence community ought to be able to give us some testable advice about any particular risk. The chance of a dedicated group of scientists someplace creating a bio weapon that can destroy humanity is remote, so you should be cautious.

Mr. SHAYS. Why do you say, it's remote?

Mr. GILMORE. It's hard to do. All of the information that our commission has gotten is that it's extremely difficult to get these weapons, extremely difficult to weaponize them and extremely difficult to deliver them. We were not prepared to rule out a weapon-of-mass-destruction attack on the United States, but in the very first year, we assessed the likelihood of a conventional attack on this country as being highly probable, the chance of a weapon-of-mass-destruction attack on this country as being highly improbable, not completely beyond the pale; and that's why we have considered it on a continuous basis as we have gone on.

Our most recent threat assessment contained in our fourth report changes that analysis not one whit. It's just very difficult to deliver those kinds of weapons, and we should be cautious about governing policy along those lines.

Mr. SHAYS. It's difficult if you are not willing to carry it yourself. But if you're willing to carry it yourself, it becomes a lot easier.

Mr. GILMORE. If you can get it.

Mr. SHAYS. There are two parts. But if you are willing to infect yourself and others who are very willing to, you know, be blown up in an airplane that hits a building, it strikes me that the reality becomes very different.

Mr. GILMORE. It's very difficult to get those weapons. It's very difficult to create those weapons.

It's very difficult to get smallpox, for example, very difficult to weaponize it. If our suggestions are put into place, particularly on the health side—which has been the greatest extent of our work, by the way, for the 4 years has been the health piece and the public health system and the ability of hospitals to deal with this—you could contain those kinds of attacks, should they occur. But they still remain highly unlikely compared to that which terrorists can

get, which are explosive devices, hijackings, attacking vulnerable points. That is very likely and has of course, been borne out.

I think your question with respect to this, I think September 11th is driving and coloring the policy decisions that the Congress is making and the executive branch is making. The threat seems so much more real after September 11th in terms of the potential attack, which then leads us to the analysis that if you allow either a terrorist organization or a foreign country to continue to develop these kinds of weapons, and with the visceral fear we now have in America with this kind of attack, then that leads more toward a policy of preemption, the notion being that we can't allow someone to develop that kind of weapon and put us in that kind of position.

Even if they can't get the weapon here, which they probably can't, they could get it around their neighbors, and then, in that position, upset the entire balance of a major region where the national interests of the United States are at stake. This is the analysis, I believe, of the President.

Mr. SHAYS. Thank you, Mr. Chairman.

Thank you, Governor.

Mr. TURNER. Do you have any additional questions?

Mr. JANKLOW. Let me pick up on where Congressman Shays left off on the comments that some of you panelists made.

Governor Gilmore, it's extremely difficult to manufacture these, there's no question about that. But when a State sponsors the research and the manufacturing, just exactly like has gone on historically in the Soviet Union, what has gone on in North Korea and clearly what is going on in Iraq.

I mean, we can all argue and will continue to argue what is or isn't present in Iraq. But after the inspections started back in the 1990's and after several years and after Saddam Hussein's son-in-law came out of the country and then others talked about what was inside the country, all of a sudden the world—there was an admission, there was anthrax in the country in very substantial quantities and research going on.

There was smallpox within the country. There was no candid admission, but I don't think there's been any intelligence service from any country that hasn't understood that there has been smallpox research going on in Iraq.

Clearly, there was research with respect to risin and some of the other types of weapons of mass destruction.

You don't have to wipe out the human race in order to wreck it, especially when you live in as sophisticated a society and economy as we have. September 11th is a classic example of the hundreds of billions of dollars, the price we're paying for those particular incidents taking place.

Our country has had a long history of explosions: antiwar efforts blowing up buildings at the University of Wisconsin; as I recall, the Symbionese Liberation Army [SLA], back a couple of decades and explosions they were doing; things that some other groups were involved in. Europe clearly had the Red Guard and all of those types of things. Japan has had the incidents with respect to poisonous gas.

But the point is, it doesn't take much in a society to change the standard of living, to change the culture.

You keep talking about—very eloquently, Governor, about how we just have to evaluate all this and then we have to make policy decisions. But the fact of the matter is, no one who drafted our Bill of Rights, or subsequently that has dealt with it, ever had in mind the kinds of terrorism or the kinds of wanton acts that human beings would do to one another with respect to deliberately inflicting diseases and those types of things. So, I mean, we have a tremendous challenge, as you keep saying all the time, where do we draw that line?

I think hoof and mouth disease, although it has been with animals, is a classic example of how easy it is to spread—for example, smallpox is not a difficult disease to spread. Clearly, it's done by contact. But to the extent that people are as mobile as they are in today's world, again if someone is willing to die, to infect themselves with smallpox and they're willing to die, they can have a huge amount of contact with others, like at airports or public arenas, what have you, before they reach the point where they are no longer capable of being a bomb themselves.

So after having said all of this rhetoric, my question to you and to you, Mr. Krepinevich, is what is it—what is it that should be expected of us? If you're a citizen out there, what is it they should expect of us to be able to do—is there anything we can do in the legislative sense? Is it our responsibility to talk about it? What is it that should be expected of us?

Mr. GILMORE. It's a very great policy question. I don't think that the American people should expect of their legislators that they are going to provide them complete security from all imaginable attacks and terrorism. I don't think the legislature can do that. It's unrealistic to hold you accountable for some diseased mind and some idea that somebody might come forward with—and, you know, it doesn't even have to be a weapon of mass destruction. It can be a bomb in a local McDonald's in downtown St. Louis.

Mr. JANKLOW. It could be snipers.

Mr. GILMORE. And I think we have to begin to go through the education process that says that we are going to assess the risk in a realistic way. We're going to take the appropriate measures that are realistically based upon those threats, those realistic threats; and then we are going to get on with our lives and understand that we're going to live like we have always lived. And I think that's part of the answer of both expectations.

I mean it's clear that you don't have to have weapons of mass destruction to wreck a society. I think the society is on a hair trigger right now, and I think we need to back away from that a little bit.

The agricultural terrorism—by the way, I want to throw in, since you raised it, Congressman, that we have a whole chapter here on agricultural terrorism, so we are not excluding any possibility as a weapon of mass destruction, hoof and mouth disease or any other potential attack.

But we think there's an obligation to reasonably assess the threats in a realistic way. Try to avoid—in a perfect world, I suppose, trying to guard against everything for fear that if you miss something and something bad happens, then some commentator or

some newspaper is going to criticize you and say that you didn't think of that.

Mr. JANKLOW. That's what they do, though.

Mr. GILMORE. We can't think of everything. And we have to be honest about it with the American people that we owe an obligation to reasonably assess the threats, put together a national strategy and make sure all the resources of Federal, State and local people are drawn to it, and we all understand what it is, we're properly funded, not crazily funded, and then put it into place; and then build this and then explain to the American people that life has never been risk free and go on from there and ask them to live free lives.

Mr. JANKLOW. Dr. Krepinevich.

Dr. KREPINEVICH. To come full circle, again, Congress has the responsibility of the purse to provide the means. Congress is also responsible for declaring war. So I think it's appropriate that Congress pass judgment on the strategy, which essentially is, how we are going to go about dealing with this particular threat to our security?

So what does this mean? I will count off a number of things that I think Congress has to look for. One is, do we have an adequate statement of the character of the threat? Is the threat a renegade group that we're talking about in terms of international terrorism, or is it a popular movement?

If it's a popular movement, then it takes on the characteristics of an insurgency; and an insurgency is a popular movement that has got a fundamental level of support among a specific group of the population. If this is a movement in the Arab world, for example, or in the Islamic world, then it's not essentially a police action. It's an action that at some point if you are going to get rid of this brand of terrorism, you are going to have to go after the root causes of why these people are doing what they're doing.

And it seems to me their objective is to get the U.S.' influence out of their part of the world, and in a sense, to keep Americans from exporting their culture, to stop being Americans in a sense.

So what is the character of the threat that we're dealing with? What is the goal? What do we wish to accomplish? What are the means?

And, again, your responsibility is to get a sense of whether the means can actually be provided. Are we willing to make that kind of a national commitment to "X" billions of dollars year after year after year because, as we know, the President said: that this is a protracted conflict which we're in.

Preemption, strategists will tell you, buys you time. When the Israelis attacked the Osirak reactor in 1981, they bought themselves time. What do you do with that time? That has got to be a critical part of your strategy.

Metrics, again, how do we measure progress, not just in one area, but in a number of areas. But I think that is if we have these multiple strategies then we ought to have performance metrics.

Mr. JANKLOW. Don't you think—and I am cutting you off just a little because of time, but don't you think when Congress, when all of America, focuses like they did after September 11th, which we all agree was a focal point for us, and then we all agreed we need-

ed a homeland security-something, and then we get hung up and Congress goes home for Christmas and everybody just takes time off while we discuss civil service protections for people, doesn't that really—and I am not questioning the impact it has on individuals that are employed in the government. I'm not. But doesn't that really trivialize it for someone out there in Timbuktu, America, with respect to what it is, the sense of urgency we are trying to convince them we're dealing with?

And then we still haven't funded it. Now they're all screaming, where's the money? We told them we would give them the money. We're not giving them the money. Doesn't this really fly in the face of what we call a sense of urgency?

Dr. KREPINEVICH. I think certainly there needs to be a sense of urgency. One of the political wags opined that the situation is critical, but not serious and in a sense you could argue—

Mr. JANKLOW. Where I come from we call that a distinction without a difference.

Dr. KREPINEVICH. Again, the years 1945 to 1950 when we developed a containment strategy, we were not at war. We were not being attacked. We did not have military forces engaged in combat.

We certainly need that sense of urgency. And I couldn't agree with you more. The question is, what is it going to take to get that sense of urgency?

Mr. JANKLOW. We don't have it, and we expect the public to give—we are privy to folks like you coming before us to give us information. But out in the hinterland, they don't get that. They will get a snippet of this. They will get a paragraph of this in some third rewrite of an AP story.

I'm not being critical. I'm just saying, it isn't fair to them in order for them to drag their politicians to make policy decisions.

Mr. TURNER. Mr. Chairman, do you have any additional questions?

Mr. SHAYS. I would like to thank you, Mr. Chairman. I would like to thank the witnesses for their participation today and particularly to thank you, Governor Gilmore, because when we set this up, you could have asked for a separate panel. It would have made it not as interesting, and by your participating with the other three panels this way, it makes it more informative. I appreciate you not pulling rank like that.

I would like to thank the rest of you—just a tremendous job.

Mr. TURNER. Well, I would like to thank the panelists also and ask if you have any additional comments or statements you would like to be included in the record. Do any of you have any additional comments?

Mr. NEWHOUSE. I remained silent during this brief discussion, but it seems to me, rightly or wrongly, there isn't any sense of prioritizing this enormous range of threat.

The so-called "threat of terrorism" has a number of elements. And there was discussion just a few minutes ago about focusing the public—making the public more aware. Seems to me the public's attention has been focused, but it has been focused on Iraq. And Iraq is a real threat, ugly threat. The issue, really—and it's debated and there's a case to be made either way, but the case is whether it's an imminent threat, or if it isn't an imminent threat,

how imminent. Is it more imminent than say the interrelated threat from al-Qaeda and the Arab-Israeli quarrel. Or Pakistan and the interaction between Pakistan and North Korea, the fact that this technology exchange between—could result in the North Koreans selling nuclear technology to this one and that one, anyone who is prepared to buy it. It is also the case that while we are debating a lot of this, that is, to say what to do about Iraq, that India and Pakistan will shoot their way to the head of the agenda.

So there's a lot to worry about. But I myself don't get any sense of prioritizing the range of threats.

Mr. TURNER. If other members of the panel have no additional comments, we thank you again and we will be adjourned.

[Whereupon, at 4:55 p.m., the subcommittee was adjourned.]

