

Summary of Meeting – Public Session  
U.S. Department of Homeland Security  
Homeland Security Advisory Council

June 26,2006

**Meeting Summary:**

This summary describes the discussions and recommendations of the U.S. Department of Homeland Security's Homeland Security Advisory Council (HSAC). The meeting was held from 11:10 am to 12:30 pm Monday, June 26,2006, at the St. Regis Hotel in Washington, D.C.

The HSAC met in Washington, D.C. for the purposes of: (1) DHS leadership discussing with Members on the Critical **Infrastructure** Task Force's recommendations; and (2) receive briefings and deliberate on the **future** of terrorism; threat assessment for the next five years, and creating a common culture within the Department of Homeland Security.

**Participants:**

Council Members in Attendance:

Judge William Webster, Chairman

James Schlesinger, Vice Chair

Kathleen Bader

Elliott Broidy

Frank Cilluffo

Jared Cohon

Ruth David

Tom Foley

John Magaw

Patrick McCrory

Erle Nye

Lydia Thomas

**U.S. Department of Homeland Security Representatives:**

Secretary Michael Chertoff

Assistant Secretary for Policy, Stewart Baker

Assistant Secretary for Strategic Plans, Randy Beardsworth

John Wood, Chief of Staff

Douglas Hoelscher, Homeland Security Advisory Council, Executive Director

Michael Fullerton, Homeland Security Advisory Council Staff

Jeff Gaynor, Homeland Security Advisory Council Staff

Mike Miron, Homeland Security Advisory Council Staff

Candace Stoltz, Homeland Security Advisory Council Staff  
Carnes Eiserhardt, Homeland Security Advisory Council Staff

### **Speakers**

Dr. Walid Phares, Author of Future Jihad, Terrorist Strategies Against America  
Angela Drummond, CEO, SiloSmashers

### **Public Attendance:**

Approximately 40 members of the public attended the meeting.

### **HSAC Meeting Called to Order at 10:05 A.M.**

**CHAIRMAN WEBSTER:** Good morning. I would like to call this meeting of the Homeland Security Advisory Council to order and to welcome all of those who are here as part of the public session. My name is William Webster, and I am the Chairman of the Homeland Security Advisory Council, or HSAC, as you will hear it referred to in discussions. I would like to welcome our members and the guests that we have here in attendance.

For members of the public who are unfamiliar with the HSAC and its charter, this Council serves to provide independent recommendations to the Secretary of Homeland Security across the spectrum of homeland security efforts.

On today's agenda, we will be receiving and discussing the Secretary's two new initiatives for us: one, the future of terrorism, looking ahead five years down the road; and, two, building a common culture within the Department of Homeland Security.

To support these efforts, we have with us today Dr. Walid Phares and Angela Drummond, CEO of SiloSmashers.

Dr. Phares is the author of the book Future Jihad, which many people are reading with a great deal of interest. I know that what he has to say will be of importance to us.

Around noon Secretary Chertoff will be arriving. He had planned to bring Senator Susan Collins of Maine, but she, like many other people, is having transportation problems due to the rain. She will be here later today, but whether or not she makes the public session is yet unknown.

Before we begin our discussions on these two new areas of focus for the Council, I am pleased that Assistant Secretary for Strategic Plans, Randy Beardsworth, is with us this morning to discuss the important concept of [critical **infrastructure** and national] resiliency and the ways in which the Department is implementing it.

I would certainly like to thank Dr. Ruth David for her important work in this area as the Chair of the Critical **Infrastructure** Task Force.

The Task Force's recommendations provide the nation an empowering, risk-based critical infrastructure objective that is resiliency and an objectively measurable and universally understood metric of time to manage its achievement.

And, with that, I'll begin the discussion with the members of the HSAC. I would like to ask the Department's Assistant Secretary for Strategic Plans, Randy Beardsworth, to discuss the implementation of the recommendations of our Critical Infrastructure Task Force.

**ASSISTANT SECRETARY BEARDSWORTH:** Thank you very much Judge Webster. I am pleased to be here to talk a few minutes about resilience and to engage in a bit of a discussion for a few minutes before our other speakers.

I was pleased when I saw the HSAC [Critical Infrastructure Task Force] report that the number one recommendation was to promulgate critical infrastructure resiliency as the top level strategic objective, the desired outcome to drive national policy and planning.

The HSAC's Critical Infrastructure Task Force Report defined resiliency as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade **gracefully** when it must.

The concept of resiliency is growing, not just in our country but around the world. The British had certainly been talking about resiliency in their planning, and we have begun thinking about resiliency in similar terms.

Traditionally, if you talked with people several years ago about resiliency, they were speaking in terms predominantly of recovery and how you recover and how you plan to recover from an incident.

Both the HSAC and DHS in its thinking realize that resiliency is a systems approach. And more and more in **everything** that we're doing, we're viewing the work of the Department of Homeland Security in terms of systems.

As we have been developing our strategic plan, we're convinced that resiliency should be one of our key goals in the strategic plan. As a start, we recognize the resiliency must include the concepts of preparedness, response, and recovery. It needs to include all three of these elements.

But it's even more than that. As the HSAC's Task Force report also points out, there's a psychological dimension to resiliency. And from a strategic perspective as we deal with resiliency, we need to recognize this dimension.

It means that our public has confidence in the nation's ability to be resilient. It means that we have a mature understanding of risk and that we view risk in a rational way. It means not making anti-resiliency-type decisions in the heat of battle.

There have been a number of [national] exercises and tabletop exercises over the last three or four years where we have found that it's very easy by our own actions to take a system offline, but it's increasingly difficult or very difficult to bring systems back online. And we need to recognize this and not make the wrong decisions that are going to keep us from being resilient.

And, at the same time, we need to exercise in our national exercises the idea and the concept of resiliency and pay attention to resiliency. These are **things** that we are already beginning to do within the Department and within government.

As we write our strategic plan, we're **trying** to provide the over-arching strategic guidance to the Department to emphasize and weave resiliency into all aspects of critical infrastructure, preparedness, response, and recovery planning and to provide the strategic umbrella of resiliency that the HSAC report calls for.

I hope Dr. Ruth David would like to make a few comments on the HSAC's Critical Infrastructure Task Force report.

DR. DAVID: Thanks, Assistant Secretary Beardsworth. Let me first say I am delighted to see the Department picking up the work of the Task Force and extending it. I am very, very happy to see the elevation of resiliency as a concept even above the critical infrastructure, **which** was our chartered focus of the task force. But, as you rightly point out, resiliency really is the higher-level umbrella. And I **am** also delighted to hear you speak so eloquently to the psychological dimension.

As we were discussing a little bit earlier, if one steps back some of the recent events and characterizes the cost to our nation of the event itself in terms of the immediate impact, whether it's the devastation and lives lost, but then does the second calculation, which considers the second and third-order effects, the behaviors that change, the industries that were impacted, that is another measure of resiliency that I think we can look at because hardening the psychological target in a sense, breeding more resiliency into our population may well help mitigate some of those second and third-order effects.

I believe very strongly that resiliency is the umbrella goal, the desired objective, and that preparedness, prevention, protection are all strategies to **achieve** resilience. None of them work in isolation. In fact, in isolation, any of those strategies are brittle in a sense. But if you cast them all toward the desired goal of resilience, I think we'll truly advance the state of planning in the nation.

I will say since we published the report, I have spoken to a number of different groups in regions where communities are very keenly interested in I'll say continuity of life in the local community, while the private sector is keenly interested in continuity of business. All of this is a move toward resilience as the planning objective.

So I heartily endorse this approach that you're adopting with a strategic plan and believe that it will begin to align the vectors of action of a lot of these disparate stakeholders' groups.

And I think that is the only way we will move the nation forward.

So thank you for your leadership. I'm delighted to hear it.

**VICE CHAIRMAN SCHLESINGER:** How are you doing on resiliency in non-terrorist events?

**ASSISTANT SECRETARY BEARDSWORTH:** I think that is one of the many aspects of resiliency. Specifically I wouldn't be able to give you a direct answer to that now, but that is certainly one of the things that we were talking about just as we came in here as a tremendous example. We have tried to expand that out beyond to include all-hazards. And that is true of resiliency, too.

Dr. David and I were having a conversation about - is resiliency just focused on terrorist issues or is it on non-terrorist-type issues? I had postulated that perhaps from the non-terrorist area, we have been historically been fairly resilient.

And then there was discussion back and forth that perhaps there are certain areas that are catastrophic that we haven't been near as resilient as we should be. The resilience objective has to include those areas. We specifically used the power grid as one of those areas where we need to ensure that we have the right operational resiliency standard.

**VICE CHAIRMAN SCHLESINGER:** We know it's not just the power grid. The power grid goes down. You don't pump gas. The pipelines don't work. The sewage system doesn't work. You don't deliver water. Almost everything is dependent upon delivery of electricity. When one talks of risk and resiliency - that looks to be a very prime, hi-consequence target.

**DR. DAVID:** If I could add just a little bit to that, Dr. Schlesinger, one of the things we noted in the report and Randy pointed out as well is resiliency causes you to take a systems perspective to identify those interdependencies very, very explicitly and to understand how one outage affects others, even in the aftermath of Hurricane Katrina, when we were experiencing fears of gas shortages because of pipeline and refinery disruptions. Those are all the cascading effects that accompanied a major catastrophic event.

So resiliency really does cause you to elevate and take a systems-level perspective, and understand those interdependencies in a way that protection strategies in isolation, for example, may not.

**EARL NYE:** Dr. Schlesinger, I suspect your question was just illustrative of others, but with respect to the electric power grid, I guess there's good news and there's bad news. Of course, the grid itself is designed to accommodate a certain number of independent acts that might jeopardize the reliability of the system.

We've had a couple of exceptions to that resiliency, '03 and so forth and so on, but there is a good bit of work ongoing in the industry itself and generally through the sector partnership

to recognize that the kind of planning, the kind of resiliency you build into the electric power system for acts of God, for accidents, and the customary nature are quite different from what you have to build in for acts of terrorism.

And there are steps being taken -- and I won't get into any details -- to provide a greater degree of reliability and greater degree of resiliency and a greater degree of recovery, which, of course, gets to be very critical from the economic point of view that you pointed out.

I would say also that in the National Infrastructure Advisory Council, which I represent here, there is an ongoing study of interdependencies, to which you've alluded. And that is, it's apparent, but it's very complex. And it's deeply embedded in our society, and it's something we're trying to get a handle on. And certainly the whole idea that we can make that perfect is not possible, but we do think we are making real progress. And hopefully our report will be helpful as well.

**JOHN MAGAW:** Mr. Chairman, a rather simple statement but I think a very important one, but I think it goes to the culture of whatever organization you're dealing with. It doesn't make difference how small or how large it is.

Resiliency must be embedded in everything that you do, must be embedded in your vision, must be embedded in your mission, and it must be embedded in your values. If it's embedded in those three things, everything you do will have resilience in mind.

**DR. DAVID:** I think that is very well-stated. And I would only end with an offer to Randy -- if I can be of help in what you have taken on because I recognize the monumental nature of the challenge. So if I or my Task Force members can help in anyway please let us know.

**ASSISTANT SECRETARY BEARDSWORTH:** Thank you very much. The idea of resiliency seems self-evident, but the complexities of it, as Erle mentioned, are sometimes hard to fathom. And where we need assistance, one of the areas, is to ensure that people understand the importance of resiliency and what it means and that it is a systems approach.

This is in some ways a new concept for the government to get their arms around. So we appreciate the Task Force acknowledge the importance of resilience in critical infrastructure. We look forward to the partnership to try to move this concept forward.

**EARL NYE:** Mr. Chairman, it seems to me we ought to acknowledge Dr. David's substantial contribution in this area. I followed her work on this; an overwhelming kind of an issue, of which they took on the sum bigger and I think delivered an outstanding report. And I think we owe her a debt of gratitude and her team.

**CHAIRMAN WEBSTER:** I'm glad that you made that observation. And I was certainly going to follow through because we could talk a lot and write a lot of words, but occasionally a vision emerges that's simple and clear and we can apply the test against every aspect, as the Secretary said, of what we're doing to see whether it supports that end goal. And we are all very grateful for your help in pulling this together.

Thank you. I think we'll move on now to a discussion of one of the two assignments that the Secretary has given us to think about, the first of which being the future of terrorism.

And we are particularly fortunate to have with us Dr. Walid Phares, who is a recognized expert on terrorism and Jihadism. He is currently a terrorism analyst and MidEast expert with MSNBC, CNBC, and NBC.

And we're looking forward to hearing. I realize that you can't summarize what's in this enormously interesting book, but we are grateful for your time and whatever you can share with us. And we'll have some time for some questions afterwards.

Thank you very much, Dr. Phares.

DR. PHARES: Thank you, Judge. I would like for also to thank the Department of Homeland Security for extending this invitation – and the team that helped me put together this summarized, condensed presentation.

Most of my remarks today are covered in the book, Future Jihad Terrorist Strategies Against America. What I would like to do is draw your attention on the necessity of thinking wider.

Five years after September 11th and, of course, about 15 years after the Jihadist movement engaged in a **confrontation** with the United States and the West, it is time now to reflect upon the future, meaning half a decade, one decade, and beyond, in terms of ten major questions that I have put forth here.

The first question, which seems to be very simple, is the United States homeland security targeted strategically? And what I mean by "strategically," is there a **thinking** process among the terrorist networks, the center of which would be the Jihadists but not exclusively? Is there a thinking of going after the national security, national economy, and demography of the United States in the strategic -- is there a plan is the big question because that would indicate to us in terms of homeland security, what would be the counter plan?

Instead of going only **after** the cells that we can find, can we meet those cells as they develop? Can we, of course, correct our strategies with regard to shielding our infrastructure, meaning **thinking** inside the mind of a Jihadist or of the terrorist organizations on a strategic level?

Number two, consequence of the first question, is there one strategic enemy to national security? Are we talking about -- and this is very relevant, in light of the various arrests over the past six months, one year of different types of groups: self-declared, not declared as Jihadists or what we call them today, the homegrown? Are the homegrown really only homegrown or are the Jihadists homegrown? Will that make a difference at the end of the day what is their final view and vision?

Number three, how long has the war against the United States been going on?

I take us back to the discussions by the 9/11 Commission, which basically tried hard to find out when actually al-Qaeda was born and, therefore, in reflection, when did it start its activities within the United States so that we could, like in any other science, look at their median range, long range strategic objectives, as I will discuss in a minute or so.

So it's important to determine, to reread a little bit the history of the "enemy" of these federations of organizations, their views. How did they assess 9/11 is very important because that assessment is going to tell us what is the next range of attacks against the United States.

It is very important I think in my own modest contribution to understanding terrorism we need to know where they are, what do they want to achieve in sending a second wave of Mohammed Attas to accomplish another type of 9/11. That would affect our immigration policy. That would affect transportation policy.

Would they rely on already inserted cells, which basically are citizens and, therefore, have the protection of laws? That would open a different view of what we should do and how to preempt that.

The third wave that is also of great importance after the arrest obviously a few days ago in Miami of a group that we are still looking into the ideology of, would that generate what I call in my book mutant Jihad, meaning groups who have not been educated or recruited directly by al-Qaeda but could be potentially? Where would we start to begin to meet that threat in the future?

Number four, what were the strategic objectives for 9/11? I know this is going backward, but it is important to reread this carefully. And I am among those who are really trying to understand what was on the mind of, let's say, bin Laden but others as well.

Was it to provoke mass killing only? Was it to provoke mass killing leading to mass rioting? Was it to provoke another series of attacks projecting that other cells would have responded in other waves? That is really important as well in determining the future of terrorism.

Number five; are there new strategic objectives since 9/11? We are working on the assumption that any future attack is going to take the dimension of 9/11 using potentially transportation and communication, but our imagination would widen more and more if we look further into the details of what is it that, let's say, specifically the Jihadist movement, which is not one-dimensional -- it has multiple dimensions -- wants to achieve.

Do they want basically to bring down national security inside the United States to achieve goals in foreign policy? That is one perspective. Would they want to achieve the basis for a long urban disturbance within the United States, a sample of which I have seen in terms of discussions in chat rooms and, of course, in the documents released after the several arrests, let's say, in the Florida case, Miami, in the Virginia case, in the Oregon case?



All of these have a lot of indications for us to look into the future, which may not be of interest immediately to the public now or to the legal process. Meaning what we look at in court is a way to indict, and we analysts look into those fragments of information to determine if there may be a third or fourth wave coming.

For example, the media was extremely interested in knowing in the case of Miami - is that a case that would mushroom? What are the components that would create similar cases around the nation, if not beyond?

Question number six, quickly -- and, of course, **this** is a more critical one, more sensitive one -- how deep and wide is the Jihadi penetration in the United States -- this would be a central question in any homeland security thinking for the future -- is their first penetration? Can we define what is a penetration, meaning people who do want to harm the United States, who are not actually involved in the direct mechanism but are thinking about organizing for.

Homeland security traditional perspective would go **after** the terrorists once they would involve themselves into what they call the legal studies conspiracy, too. But homeland security on a national historical strategic level would want to look at the previous 90 percent of the process that would bring the terrorists to decide that they want to go forward in that process in the future.

Number seven, I thought of another also unusual question. There are immense energies that have been developed by homeland security since 2001. The question is, is homeland security really disrupting the Jihadi penetration? It's a fantastic question.

Are our actions really disrupting other than arresting the cells? Of course the answer has to be yes -- but the other question is are our actions shielding industry? In shielding the other areas, critical areas, of our civil society, are we disrupting that? And there are indications that we may be. There are indications that we could do much better in the **future**.

Number eight -- what are the future goals of the Jihadi networks, practically speaking?

The big question which comes to the mind of both media and academia is why aren't we seeing a similar 9/11 operation? **This** is a very important question.

The answer to that rests in how the Jihadists want to accomplish their objectives. I'll give you an example: A and B. And these are just theoretical projections.

**A**, perhaps the next strike that the same organization, in this case al-Qaeda, wants to administer has to be of the dimension on a greater dimension of 9111. That's one important theory.

The second theory, maybe the next wave is not going to be of the type of one major strike but of unleashing within the United States a mechanism that would produce waves and

waves, meaning you would need to have the demography of the terrorists, the demography of cells able to unleash a second wave, a third wave, scenario, which I have developed in chapter 13 of the book, meaning what would have been a successful 9/11 operation had al-Qaeda waited five or six years, been able to penetrate deeper and wider. And I, of course, provide the details in the book.

Number nine, where and when should the interception occur? Now, we don't need to be political scientists to figure out that our interception now in homeland security for obvious reasons occurs in the last ten percent of the process, meaning when the conspiracy or the members of the cell or individuals begin to start their mission.

I think we need to begin to **think** about intercepting earlier in the process -- and I will show you a model at the very end -- intercepting earlier in the process, at least from 50 percent, if not 40 percent, of how these Jihadists become Jihadists. That's less expensive and obviously will better defend homeland security in the future, which will be the answer to number ten, suggestions for specific **counter-Jihadism** strategies that would locate, **identify** the area of spread of **this** ideology.

If you look at the entire literature of all Jihadist organizations, Salafist, to start with, you would see that they have a common objective. That's, of course, not affecting homeland security directly. It's a new caliphate. But what would that mean?

If every single individual from Virginia, Miami, to Bangladesh who is involved in this new caliphate buildup are working, if not connected organically but working in the same direction, look at the huge effort that Jihadists would want to put in the next 10, 20, or 30 years, if we look at the **Sunni** triangle in Iraq today, at the conflict we're involved in Afghanistan as major areas of deployment and we find this overstretched, -- we do find this, and it is overstretched -- look at what lies ahead in the mind, of course, of the Jihadists, it doesn't mean that the United States is responsible for obstructing **this** establishment of a **mega-Taliban** state, but it means that in the mind of the Jihadists, in order to establish this virtually in the future, they will be engaged against 50, if not 60 countries, which is the war on terrorism seen **from** their perspective.

Now, in order to establish that future caliphate, they are engaging in several battlefields against the United States and against the allies of the United States. This is just a little example of the span of the areas of confrontation. It is much wider today, three continents.

So most of the concentration of the Jihadi terror was on Europe, Asia, **Africa**, and South Asia areas. And the United States for 20 years, at least until the '90s, was not hit. And there are reasons for that.

They considered the United States an area to raise funds. They were to engage the United States in 1993, first New York attack, and, of course, 2001, 9/11. Now, **from** 9/11, things change for us and things changed for them. The next map will show you the U.S. strategies seen by the Jihadists.

There are three major components. If you are a Jihadist on the chat room or elsewhere, you would see that the basis for your strategies comes from the mainland, establishment of United States homeland security.

US homeland security is the basis for two offensives. One is the war on terror, where we are engaged around the world. Second, probably as important, if not more important, for the Jihadist spread of democracy is the so-called war of ideas.

Now, if you are the Jihad leader, not just the rank and file, and you want to defeat the two arrows; that is, the war on terror and the spread of democracy, you would hit the base. You would have to hit the base.

Therefore, hitting homeland security to the Jihadists worldwide is of a crucial nature. This is why they, the Jihadists, have a concentration on, if you can show the next one, strategies of Jihadism in America.

In our discussion, usually we go to the last one, terrorism, meaning where are the cells going to be **striking**, what should we defend, what should we shield. In fact, in my book and in other research I've conducted, terrorism is the last, the very last, stage of the Jihadist movement.

The first stage is political, not in the sense of democratic political -- of elections and on elections. It's basically establish in the war of ideas waged by the Jihadists a shield that would minimize the attention of the public, that would discourage the government in looking very early to the process of the Jihadists. That's the war of ideas engaged by them.

Of course, I developed this into a variety of ways. How do they do it? We call it in America lobbying. They call it basically political activism. That is very important. It is critical. It is difficult because it is done under the legal system.

Ideological is a second step whereby they aim at producing two things. Within our educational system -- and I will develop this further if there are questions -- there are mechanisms today -- and it has been in practice for the last 10 to 20 years -- of deflecting the attention of our talents, meaning from the classroom all the way to the newsroom, all the way to the war room, all the way to actual public America of minimizing the threat of Jihadism.

If you minimize the threat of Jihadism in the mind of the public, then when Jihadism will emerge, you will only see it at its final stage, which is when it will strike you.

Third level, urban Jihad. Now, if we look at the variety of arrests done in the United States and of other cases not ending with arrest, you will see, and I can establish a map, more or less, that the ultimate objective of the Jihadists of al-Qaeda and other groups is to create within every single major agglomeration an entity of urban terrorism that would have in the future, when it will become consistent, a capacity of paralysis, a capacity of creating havoc within each one of these cities. This is a **long-term** strategic plan which has been applied in

a variety of places around the world.

Now, if you take examples from the U.S., from Europe, and from the Middle East, you combine them, project them, the model of a sniper, the model of a dirty bomb, the model of local militia -- I call them terrorist militias -- forming, even without these individuals knowing that they are going to be part of a much wider deployment.

In the future when they are connected by the mother ship, they are part of a big puzzle that we need to begin to see, meaning to have hundreds and hundreds of not necessarily very professional Mohammed Atta-like Jihadists, meaning those who come on a mission from abroad, but individuals from within the national tissue.

The French, for example, were very interested and continue to be interested in what could be below the structure of urban disturbances that occurred last fall in France being able to paralyze about 200 cities, burn 10,000 cars, of course, for socioeconomic reasons, but what if. And that's what the French are interested in knowing now. There is a Jihadist mechanism that could do the same testing, paralysis of national security but with weapons and with violence.

Number four is the most professional work, I guess, of a potential future terror network that would at the end of the day lead to the strategic objectives.

Penetration is basically infiltration, on the one hand, meaning silent Jihadism, an individual who has the same beliefs, who is sophisticated and educated, including our system, would be able to withstand and be patient enough for five to ten years. And it's something that any nation fighting terrorism was and will be and should be aware of.

The phenomenon of penetration of the system means that at some point in time, any homeland security, of course, from a security perspective and from the technical perspective should project that elements from the Jihadi element would go as high as possible, would want to go as high as possible in the organization/apparatus so that it would in the future relate information, in the future block decision-making mechanism, and effect the national security.

And, finally, terrorism, because that is the last stage helped and aided by the other four levels. Obviously to summarize quickly, the Jihadist terrorist strategy, which comes at the very end of the process, has the luxury and the discretion of choosing their targets.

Now, we are running, as a nation to try to secure these targets, assuming that these would be the targets. And we are basically spending billions and, rightly so, rationally so, except, of course, discussion on where and how, which is not my field.

But if we are in the mind of the Jihadists, after all, what I have described until now, what is it that they would target so that they would achieve their strategic goals, which is affecting national security, which would affect foreign policy, which will continue for a long term to minimize the capacity of the United States in intervening abroad and blocking their project?

Projected Jihadi terror targets. If we look at this picture, we will see a number of projected areas. And let's not be surprised or get panicked about areas that we have not seen yet, but if you want to look at future terrorism, combining examples not just from the United States but **from** intelligence; from reading chat room discussions; and, of course, **from** other countries' examples.

Domestic security is the most important one, the largest one. And what I mean by "domestic security" -- we could have another chart for that alone -- is what we all can project starting from economic and financial. I mean, there are subdivisions, which I have not introduced in this scheme because we are very familiar with all of these divisions. Tourism is an important one, banking, industry, transportation, communication.

These are traditional areas of what we consider are going to be or would be targets. But -- and here there is a condition -- there need to be enough demography of terrorists to secure an all-out destabilization process against domestic security. Let me explain this in their terms.

In domestic security strategy, in order to perform an operation on behalf of a large organization, you need to have the follow-up, the various waves. If the various waves are not ready to move in, you don't do the first wave. You don't spend the next 20 or 30 Mohammed Atta types. You would wait for what we call here homegrown, what I call local waves to be ready.

In terms of domestic security, you have also the actual infrastructure that I know homeland security and all of the other related departments are putting in tremendous time to work on.

A large organization would not start the process of harming citizens, which should be our soft belly and could be done very easily before having the numbers, but I rush to say that we have to be very careful and make a distinction in Jihadi terror targets between what could be individual homegrown elements, not even controlled by the mother ship, who would on their own as a result of what I call Jihadi rage proceed to the assassination, killing, harming, et cetera. And that is a process which is still ahead of us, not behind us. We have not seen this yet. Some claim it did happen, but it could be ahead of us.

What would encourage **this** basically would be **further** general strikes. Global strikes would involve individual Jihadi to go ahead and do what they have done, examples in Israel, in Turkey, in Iraq, and in other places. You have this **kind** of direct attack on citizens.

Obviously and finally, you have what I call classical future terrorists' possible targets, one of which is U.S. military. U.S. military is a direct enemy of the Jihadists. It has to basically be factored in their view as future potential targets.

And next to U.S. military, you have overseas deployment. I wish I had more time, but let me just throw in what would overseas deployment of U.S. military mean if targeted **from** within the homelands. That is not U.S. deployment in Iraq and Afghanistan fought by Jihadists

locally. That is Jihadists infiltrating the United States apparatus, including the military apparatus.

So that from the homeland that could affect operations of deployment in terms of **information**, in terms of future deployment, one case from just before the invasion of Iraq in Kuwait, the military who threw grenades -- this is one example of someone from inside the machinery acting outside in the variety of task forces that exist around the world.

This is not something just of projection. Chat rooms have basically discussed the feasibility of having elements infiltrating U.S. military in overseas deployment.

The most dangerous of all, of course, is the nuclear sites and what comes with it. It has a whole discipline and logic of when would and how would and what would be the objective of damaging; hitting; paralyzing, if possible, at some point in time, causing explosions in nuclear sites.

It is too large to summarize in less than a minute, but my take on **this** quickly -- is that there is a logic for the nuclear Jihad. It is not out of logic. It is not just to cause tremendous effect in the United States.

There is a specific logic. Part of it was even discussed in public in several speeches by Osama bin Laden, including in the Fall of 2001. There is a rational choice approach to when and how to use those components.

There are two trees. Each tree has its own logic, its own interests. The al-Qaeda tree has a logic of basically doing it whenever they can acquire the target and, if I may add, since we are looking into the future, the potential possibility of having Hezbollah as a new enemy of homeland security in the future if it goes bad with regard to Iran and the United States.

This is **something** that is inescapable. We need, homeland security needs, to look at potential Hezbollah possible activities. And Hezbollah is more disciplined. Hezbollah is more linked to a regime. And, therefore, the whole strategy of Hezbollah would be different.

The two areas that have not been, fortunately, hit yet in the United States but in other countries are intellectuals and politicians, but we have to be careful if we want to project to the future.

Dissidents among those who criticize the **Jihadist** movement in Europe or in the United States are and would be potential terror targets. We have one example **from** the Netherlands: van **Gogh**. But that's just one example that we need to be attentive to in the future.

Politicians over the past year, at least, many statements were made at a variety of places by international Jihadists, not local Jihadists, but that is important to take into consideration,

that decision-makers, especially in a democracy, are important in the defining of a strategy. And the rest would be logical conclusion, which leads me to my last concept of counter-terrorism interception. That is, basically, choices that homeland security and national security in general terms will have to do both in the United States and most other democracies.

At what stage, basically can we -- and I know we have all of these barriers of financial, administrative, cultural, and, of course, legal intercept the coming arrow of the terrorists. There are various stages. I mean, all terrorists have to have an ideology of the sort before they become terrorists or leading them to become terrorists. Otherwise they're not terrorists. They are common criminals or nuts.

And all of those ideological, radical elements who want to become terrorists and hit the homeland security at some point in time are part of the society and are targeted by organizations, institutions that provide that literature and provide basically the intellectual recruitment.

So we clearly have three stages here. My question is -- and it's a question of a thinking process for the nation, both the legislative level and intellectual level and, of course, the government level -- at what stage we want to intercept, can we intercept these terrorists?

The first arrow shows you that currently our homeland security, for all the obvious reasons, wants to stop the terrorists from hitting the homeland security.

Another arrow, potentially projected into the future, some Arab governments, some in Europe are now developing strategies to try to remove the ideological components that would render a Jihadist a terrorist. I could expand on that. I will give you just one term, which is "tech fear."

Plenty of intelligence services, government people around the world are trying to establish this experiment, meaning convince or deflect the attention or remove the terrorist component, **as** we call it, the war of ideas, before it becomes.

And then, even **further**, that has to do with public education. It has to do also with homeland security public education that would help individuals as such or collectivities, not to get to the stage of becoming Jihadists and, therefore, terrorists, which includes **as** a recommendation, one of the recommendations, to increase the teaching, the actual teaching, soft combination of nationally based programs on homeland security issues and on terrorism issues, where we would start very early in the educational process, which we don't have now, unfortunately, in America or in many other democracies. But this could be devised for the future.

With these remarks, ladies and gentlemen, I would like to thank you very much for your attention. Thank you very much.

CHAIRMAN WEBSTER: Thank you very much, Dr. Phares. We'll be cogitating your

remarks and extending them into the discussion this afternoon. You have a unique approach. It was very interesting, and we appreciate your sharing it with us.

I want to keep up with our schedule because the Secretary will be here shortly and turn to the second half of the challenge which he gave us, and that is to consider building a common culture.

We're very fortunate in having with us to direct this in the right way Angela Drummond, the President and CEO of SiloSmashers, a ~~firm~~ that she established in 1992 to provide collaborative management consulting services to the public and private sectors.

We are very happy to have you with us, Ms. Drummond, and I will turn it over to you now.

**MS. DRUMMOND:** Thank you, Judge Webster. It's my honor to be here this morning to engage in a conversation about something I believe so passionately. And that is looking at organizational cultures and how to build a common operational culture within DHS.

Capitalizing on what we just heard, I think all of you are probably looking inside and saying, "Do we need to change at DHS? Can we respond to the future of Jihad? Can we respond to the future of terrorism? Can you respond to what Mother Nature is going to bring us in the future?" I don't think that you would ask me here today if you didn't **think** that some change was necessary within DHS.

A lot of that change, the real big question here is, can DHS respond to these future challenges based upon the current operations, the processes, and the culture of today? And I think the answer is no. You asked me here today to talk about how to change cultures or change the culture at DHS.

And I don't know if everybody has had a chance to review the human capital survey back in 2004, but I will give you three of the areas. Only four percent of the DHS workforce felt that creativity and innovation were rewarded. That's a pretty low number. Twelve percent said that they are encouraged to come up with new and better ways of doing things, another low number. And next to lowest, employee morale throughout the federal government. So what part does culture play in that? I believe it's a big part.

Culture is defined many ways, but basically it's the unique personality and characteristics of an organization. So I challenge you again. Can DHS in the culture that is there today respond to the future of terrorism and other catastrophic events?

DHS espouses some strong core values: integrity, vigilance, respect. There are some beliefs that were laid out in the 2004 strategic plan. Today I heard critical infrastructure resiliency as the top level strategic objection, the desired outcome to drive national policy and planning and I don't see that in there. So I think that is one area that would need to be focused on.

I ask you, how do the actual values that are listed today and in the strategic plan tied to the



actual operations, behaviors, and culture of the organization today? Is there a disconnect? No wonder there is a disconnect. And I think you all are answering yes, there might be a little bit of a disconnect.

DHS is experiencing many challenges. You know, I don't need to tell most of you that. You know that. But with a large organization, as many people as there are in it today, and as important a mission that the DHS has, along with these challenges, there's no wonder why the culture needs to be changed.

So for this afternoon, we're going to engage in a **conversation** to talk a little further about the challenges at DHS, what part culture plays in that, what makes it so difficult to change, what can be done, and what are some of the next steps.

So I **am** looking forward to a more detailed, in-depth discussion this afternoon. And I thank you again for inviting me here today.

**CHAIRMAN WEBSTER:** Thank you very much, Ms. Drummond. I understand the Secretary is here and I forgot to welcome Assistant Secretary Baker. Mr. Baker, I **am** glad you're here. Dr. Phares and Mrs. Drummond have given us an eye-opening beginning for discussion of the two charter issues that you cast us with.

And we would like to turn the floor over to you now and Stewart Baker if he would like to have something to say.

**SECRETARY CHERTOFF:** Well, thank you, Mr. Chairman. First of all, I want to thank you for agreeing to serve as Chairman and Secretary Schlesinger for agreeing to serve as Vice Chair of my Homeland Security Advisory Council as well as I think we have a couple of new members who are present. Your service is very valued, and your continued participation is very valued.

In talking about the issues which I have requested the Council to address, I have tried to reflect back on the last year of getting reports and to try to think about those areas where I thought this Council could add particular value.

That tends to be not necessarily so much in short-term projects, although there's a lot of value there, too, but what I consider to be long-term strategic projects, things that are going to result in framing our strategy, not over the next six months or a year but over the next five years.

We are at the stage three years, a little bit over three years into the life of this new department to talk about how we can institutionalize some of what we have done and put ourselves in a position to deal with the long haul in the war against terrorism.

The two particular issues which I have raised or we have raised today I think really fit into that model of strategic issues. Let me just give you a little bit of an insight into what I am thinking about so you can carry that forward into the discussion today but also in your work

until we get your recommendations, hopefully this fall.

The first has to do with the future of terrorism. The fact of the matter is there is a natural human tendency to fight the last war. And that is particularly true when the memory of the last war is very vivid in our own minds. And we certainly have no difficulty in remembering with enormous pain what this country suffered on September 11th.

Nevertheless, as we look forward, we cannot assume that the model of September 11th is the only model. In fact, I would dare say if you went back to the 9/11 Commission report, you would see one of the observations they made was that prior to 9/11, we were busy focusing on our experiences in the '90s, which were for the most part, although not exclusively, attacks overseas, attacks with truck bombs. And, therefore, there was a failure of imagination when it came to an aerial attack, which we suffered on September 11th. I think one thing I want to make sure is we don't suffer from a failure of imagination going forward.

And it seems to me that, as Norm Augustine said in his little memo that he sent to us, if you look at the events of the last several years since 9/11, we see attacks that continue to be directed from a centrally based and centrally organized al-Qaeda and its allies overseas, but we also increasingly see what I have started to call virtual Jihad, people who radicalize themselves over the internet, train themselves over the internet, communicate over the internet but not necessarily by e-mail, just by interacting on Web sites, and are capable of carrying out serious attacks. I think that is one of the lessons of London and July 7th.

So what I would like to ask this Council to do is to look forward and ask what are the screens we see for the future of terrorism and what are the implications of that for how we model ourselves as a Department.

Is our strategic response to dealing with al-Qaeda-driven research on weapons of mass destruction the same as our strategic response to the proliferation of homegrown virtual Jihad?

The second issue is a little bit more parochial. We have done a lot of work in the last three years binding this Department together, shrinking the number of purchasing centers and IT centers and trying to bind together our e-mail and our IT structure and our procurement, but a lot of what forms a single department is creating a common culture and a common career path.

I thought, in particular, because this Council draws upon people with a lot of experience in business and in the private sector as well as a lot of broad experience in government, having a strategic look at how we build the Department over the next five years, how to build the kind of jointness that I think we all see as the ultimate goal of having a single department, in much the same way as the Department of Defense has learned to build a culture of jointness.

So those are my two areas that I have expressed interest in to the Chair and the Vice Chair. And I look forward to hearing your observations today and also to getting the benefits of

your study of this topic over the course of this year.

**CHAIRMAN WEBSTER:** Thank you very much, Mr. Secretary. This together with the discussion this afternoon and the perspectives from outside on these two important subjects present an interesting challenge for us. We'll try to have a report for you by late November or December on where we at least see these things going.

It's very difficult to predict, as you pointed out, whether it will take an outside centralized approach, not to take it but whether it will result in it or whether we will have homegrown species. Dr. Phares was talking about some of these issues of trying to anticipate them. Perhaps we will have both.

Earlier this morning in the executive session, we had some information supplied to us by Ambassador McNamara. And I'm trying to understand how best to share the intelligence and the information that comes our way or that we have generated and how do we share it in an appropriate way with state and local responders, who are part of the picture. And we see you as the key leader for that purpose, the implementer, for those policies.

We have time for one or two questions. Stewart Baker may have a few additional remarks. I would certainly like to hear from him if he does.

**ASSISTANT SECRETARY BAKER:** I'll keep them brief so that we can have questions. Just thinking about how to produce a product that responds to these important issues, I would urge the Council to think in new terms about the best way to interact with the Secretary and the leadership of the Department. It's not necessary to produce a long report or to produce consensus.

I think we would be as well-served by a debate among the Committee members as by a single report, by a series of vignettes, rather than an effort to be comprehensive. What is important is to bring your individual expertise to bear on a real problem that we are struggling with and to give us the benefit, rather than spending too much time trying to reach agreement. So you shouldn't feel obliged simply to produce a single report that reflects the consensus views of the Committee.

**CHAIRMAN WEBSTER:** I take it you don't want to be deprived of the minority point of view.

**ASSISTANT SECRETARY BAKER:** That's exactly right.

**CHAIRMAN WEBSTER:** We heard also this morning from your Chief of Intelligence, Charlie Allen, whom I mention without detail, that he was not always in synch with the group-think but he was very often right. And that was particularly true in identification of the Iran contra issue, which he saw and smelled and was very helpful to make a record on. I would be happy to hear from any members who would like to talk. Yes?

**Dr. DAVID:** Mr. Secretary, it seems to me that looking at the future of terrorism and its

likely evolution over time is very well-aligned with your concept that you started on day one, which is risk-based resource allocation, because risk inherently accepts that we don't know precisely what the threat is.

So have you tied those together and built that as a sort of motivating more rational debate perhaps on the topic of risk?

**SECRETARY CHERTOFF:** I don't know if I can motivate more rational debate, but I agree with you. I think that one of the reasons I wanted to get this done was because I think as we think about how do we array our resources against the threats, part of what we have to think about is where are we as a federal government best advised to focus and where are state and local governments advised to focus? What are the relative strengths of state and locals in certain kinds of Jihad versus the federal government?

At one extreme, it seems to me that when you talk about sophisticated detection capabilities for WMD, that's likely to be an area that the federal government really adds value in the unique situation. When you're talking about what I call very low signature types of terrorism with very little communication or only face-to-face communication deeply embedded in communities.

I can tell you based on my own experience in law enforcement over the years, that is really where your local police have a real advantage, real value added.

So I think that what I -- and I encourage you to put it in these terms. Your view of the strategy here should really ask the question, what are the implications of this for not only risk-based counter-terrorism but for where the appropriate emphases ought to be at the federal, state, and local level.

**MAYOR MCCRORY:** I would like to compliment you on clarifying the two points that I think this very well-distinguished panel can participate in. I do want to also say looking at the future, I think it is imperative, especially with regard to the recent debate and discussion that is going on in Congress and nationally about the allocation of resources.

I know my own city has been brought into that debate by some critics, but I think it is extremely important to determine from a financial stability standpoint for our nation and for local governments and the private sector that we do look at the future because we cannot protect everything. And there's not an unlimited amount of funds.

So I think we do need to anticipate, as opposed to react, or only look at history. I would be curious, too, to get your reaction, too. There are issues of operating costs, capital costs, and also how much preventive versus reacting resources we should look for in the future and in trying to anticipate where the possible next attack or in what form the next attack may be.

**SECRETARY CHERTOFF:** Well, let me first say, I mean, in terms of a preventive versus reactive, one of the points we have tried to drive home since the Department was created is you have to look at how we address the threat of terrorism across the whole

spectrum of activities, prevention, protection, and response. And, frankly, they are interrelated.

An example I sometimes use is if you look at the question of a chemical plant, there are many ways to deal with the threat of a chemical plant. One is to have very robust prevention capabilities, a lot of guards, and a lot of cameras. And if you really are comfortable that you have done a lot to prevent and a lot to harden and protect, you may feel you don't need to do that much in terms of response.

On the other hand, if your model is a very effective immediate response to a release, that may, in fact, be a reasonable trade-off in terms of additional hardening and protection. So that you always want to look at these across the spectrum.

And part of what we have tried to do in response to the President's direction in some of the homeland security presidential directives is to build a set of pretty specific preparedness goals. And we're about to come out with the national infrastructure protection plan or of these being an integrated approach to helping communities judge what kind of choices they need to make in terms of arraying their resources against, as you point out, a threat that we can't have an absolute guarantee about. And so we have to make some difficult choices. And they are tough choices.

With respect to the issue of capital versus operating experiences, let me say, you know, we are always in a -- I said it the other day, and I'll say it again -- we are always making choices where all of the alternatives have drawbacks. There's never an easy magic bullet choice for us where we do that and everybody would agree with us.

And so we want to balance between certainly known threats but also unknown threats. It's that failure of imagination that we don't want to get caught up in.

And I bring you back to 9/11 because I remember if you look back in the '90s at where most of the attacks were, there were truck bombs. And a person who would be spending their time thinking "Where am I going to put all of my effort?" based on past performance, as they say, would have looked at jersey barriers, those concrete barriers. And, yet, we saw that they used a different attack modality.

So I think we obviously do want to pay attention to the overwhelming history of where threats are located. We don't want to have that be exclusive. We don't want to neglect to make sure that we have at least started to provide some base capabilities across the country.

In terms of the one thing I would say -- you know, when we talk about operating expenses, what we need to look at is the challenge of operating expenses. And that is at funding operating expenses at the federal level. Certainly I understand the impulse, that request that would do this.

First of all, how does that translate into a strategy of eventually being able to fund other jurisdictions? This doesn't give us a pathway to raising the level in a sustained fashion.

The second thing is, you know, when you get into personnel costs, pretty soon after you start funding personnel costs comes the completely understandable and justifiable request that we account for the way the money is being spent. And when you talk about what, for example, responders do, that tends to come along with requests for keeping time records to make sure people are spending their time on the mission. And that tends to not necessarily be a pleasant thing for the locality. It tends to lead to a certain amount of micromanagement.

So part of what we try to do is find ways to fund -- we have clearly defined goals but in a fashion that is not going to require micromanagement. And that is another consideration.

**DR. COHON:** Mr. Secretary, good morning or good afternoon.

Two questions. One on the departmental culture. We take as a given that there is work to be done yet to create the common culture. We focus on that we accept the task that you have given us. I am interested in hearing your sense of progress in this regard in the year-plus that you have served.

Second question, related to this, is one specific incident or very important specific aspect of jointness in a common culture would be the way risk is used and risk-based decision-making is done throughout the Department through its many offices, agencies. I would be very interested in hearing you comment on that and whether we're all working from the same page or not.

**SECRETARY CHERTOFF:** Let me give you an example which I think covers both of those and illustrates the advantage of jointness. I think when we approach the issue of the border, what we call the secure border initiative, what we did was we brought at least three different strands, actually four different strands of the Department together in joint activity to do an analysis of the whole system and to develop a plan that would then be implemented by a number of the components. That was Customs and Border Protection, which really mans the borders and does the ports of entry; Immigrations and Customs Enforcement, which does detention and removal investigations; Citizenship and Immigration Services, which is involved with people who want to get visas to come in legally; and, finally, the Coast Guard, which deals with the maritime dimension of the border.

And we got people working together using the Policy Directorate as an engine for joint planning -- and Randy Beardsworth was very involved in that -- as a way of building a kind of a joint planning, a joint vision of the vision that everybody would have an investment in, as opposed to saying to each component "Here is your task, and we want to measure your task based on inputs."

We talked about here is the mission, here is what we want to accomplish. Your success is defined in terms of accomplishing your mission. So that when it came, for example, to turning the corner on catch and release and making it into catch and remove, we are quite far along in achieving that. It was important that Customs and Border Protection and ICE understood the mission and what needed to be achieved so they could calibrate themselves

and synchronize themselves to work.

I think that has worked very well. And I think one way it has worked well is precisely because it forces you to think about managing risk. Once you're thinking about achieving a goal, you're trying to think of the most cost-effective way to get there.

And that is way, for example, as we have talked about border issues, we have talked about what is the right array of border patrol, fencing, and technology to lay across the border, how do we arrange and set up our detention facilities to minimize travel time and maximize return time? And all of these are features of being risk-focused, figuring out, which in a way is cost-benefit analysis.

So I think that exercise is one which has been of great and enormous help to the Department. We are now in the process of trying to drive a lot of that jointness in the way we manage emergency response.

We've got FEMA now working with the Coast Guard and working with our law enforcement components in order to again look at emergency response of something that's synchronized, not only along a number of the components of our Department but, actually, other agencies, like the Department of Defense and Health and Human Services.

So in my year here, I have seen a lot of progress. Now, we have a lot more work to do. And predictably I think there is -- you know, every department that starts up begins with **an** immediate flush of good will and **high** hopes. And there is an inevitable confrontation with reality, which involves budget and cultural change and things of that sort.

And I think we're experiencing a little bit of that now, but I think what will emerge from that I think is a tougher and more integrated Department.

So it may be a little bit of a long-winded answer, but I think both of these pieces are features of the same issue.

**DR. COHON:** That's a great answer, but it's not long enough. That's only because we don't have time. Just one quick follow-up. So this nice **successful** example on the secure borders, are we dissecting that and trying to use that as a template for other cases?

**SECRETARY CHERTOFF:** We are. And part of what we are doing is this. We have **carried** it over, for example, in the emergency response area. We have worked very hard, first of all, in the SBI context. And we're now applying this in the emergency context to build ways of measuring what we do.

And, we break the system down. We figure out how do we measure, not just measure for the sake of measuring but measure something that is going to lead to success.

It is challenging sometimes because you often find some of these that are hardest to measure very important. They're intangible or you don't have all the facts, but as we have gone at it, I

think we have gotten better at measuring, better at figuring out what to measure.

And now as we look at, for example, the way we have developed emergency response plans with FEMA and Coast Guard, we have started to build a lot of those measures measuring capabilities, too. I think that is going to ultimately be a management tool we drive through the entire Department.

**DR. PHARES:** Mr. Secretary, just a quick comment on the issue of failure of imagination that you have just mentioned, which is very important. In my research, I have developed the idea that it is also a failure of education. In the '90s, as we all know, very few knew very little about the nature of the enemy. Therefore, the imagination was very narrow.

One of the suggestions I would like to develop for the Department to think about and other departments as well is widen as much as possible the understanding of who is the enemy and what it wants to accomplish.

And my suggestion would be to think of the possibility to educate the actual law enforcement agencies around the nation on the very basic issues. That would help them in their police force, starting from the lower level all the way up to the analyst. If they have exactly how the enemy thinks, then they could develop greater energy.

And I would add one thing: the public. I have been a professor on campus for 14 years. And I do understand that providing the public with either courses or material, very basic on who is the enemy could provide greater imagination and bigger talents, if I can put it in one word.

**VICE CHAIRMAN SCHLESINGER:** Mr. Secretary, in World War II, we had the Office of War Information. Since 9/11, we have done nothing along those lines. The fact of the matter is that we would be a lot better off if we had even a small office that had authority and spoke to the public along these lines.

**FRANK CILLUFFO:** Mr. Secretary, if I could build on Dr. Phares' comments as well as Dr. Schlesinger's, I do think that as we look at this broader -- and I think you captured it very well in terms of what the roles and missions are federal vis-a-vis state and local because, I mean, you clearly do have the al-Qaeda classic and its franchisees all over the country, but you also have this emergency leaderless movement, groups that think globally but act locally. And they are inspired and reaffirmed on the internet in this cut and paste virtual world, where you do have this reaffirmation.

I am curious as to whether or not we have given some thought to how we engage in that activity, the battle space of ideas, specifically on the internet, where it becomes an enabler, every once in a while very detailed information for how they can plan attacks, communicate attacks, and other tradecraft means. But these aren't either/or. They're not mutually exclusive.

The reality is that I think we're going to face both: those that have catastrophic and have the



training and the capability and the capacity to potentially pull that off and those that are going to be much more leaderless motivated and inspired.

But the battle space of ideas on the internet I think is an important area for all of us to give some real thought to.

**CHAIRMAN WEBSTER:** One of the things we heard this morning was not to underestimate the power of the internet as applied by the current struggle. They were using it to good advantage themselves.

**SECRETARY CHERTOFF:** There's an element of that which is technical and involves -- much of which is classified. So we're not going to talk about it in here. But then there were some really challenging legal issues in this. I mean, we have always built a model of protecting speech up to the point of incitement. And, you know, that's -- incitement now is a very hard thing to define.

Now, there have been some cases. For example, I think when they prosecuted the blind sheikh in New York for sedition. That was an example of incitement in speech.

But I do think these things are -- this is actually one that I think you all need to explore in this strategic look.

**DR. DAVID:** You did give a very nice explanation tying risk together with the future of terrorism. I want to pull you back to risk again because the example you gave was inside DHS. I understand that is the immediate challenge, but it seems to me that the whole concept of risk management as it will lead to a more resilient nation means the nation needs to have a more common understanding of what risk means.

Is there something that you're doing in that area? Is there a way that we can help in that area?

**SECRETARY CHERTOFF:** I think this is maybe the most important thing we can do in this Department in terms of how we go forward in the war against terror, which is going to be with us I think, regrettably, for years to come. And that is to build a way of dealing with this issue that allows us to go about our daily lives without sacrificing our civil liberties unduly or without sacrificing our prosperity but materially raising our level of security.

A lot of that is a process of public education and public information. And it is not an easy educational process to undertake. And in the year since I have been on the job, I have actually come to recognize it is even harder than I thought it would be. And I thought it would be hard when I took the job. And I said it would be hard. And I proved to myself that I was wrong. It was even harder than I thought.

I read a piece in the paper today that accused me of being maybe unduly frank about these issues and offending some people. And I thought, well, you know, that really is a big part of

what I hope we can do in this Department.

I do think it is -- in the long run, if we suggest to people there is a magic bullet solution or that what we ought to do to use a common example is physically open every container in order to make sure somebody doesn't smuggle something in, we will kill ourselves. We will do the enemy's work for the enemy. The enemy is actually very explicit about wanting to do this to us.

So managing risk means being clear that we have to look at consequence, vulnerability and threats. We have to make some difficult cost-benefit analyses. That's not to say we don't want to materially raise the level of protection.

You know, one good statistic I will mention to you is we are actually ahead of schedule in terms of our deployment of radiation portal monitoring and scanning equipment to scan containers that are coming into the country. We will be I'm told by approximately October 1 by 80 percent, which is faster than we thought we would be. And that is a huge step forward. Now, it is not the end of the analysis, but it is a way to increase security with balance.

I think what I would ask you to do and one of the reasons I wanted to have this strategy piece done is I think this requires a lot of discussion. I think over the long run, I actually do think most people will be comforted by an adult, realistic statement of what we can do and what we can't do and will appreciate -- and maybe I am a little too frank sometimes -- but they will appreciate candor, as opposed to being patted on the head and told "Everything is taken care of. You know, we're going to do everything."

And so that is something that you as community leaders and leaders of the government and the private sector can really play a big role in.

CHAIRMAN WEBSTER: Thank you, Mr. Secretary. We have concluded the public session of the Council's meeting. If there are any members of the public who wish to submit comments to the Homeland Security Advisory Council you may do so by sending us a letter or on inquiry.

The address is Homeland Security Advisory Council, U.S. Department of Homeland Security, Washington, D.C., zip code 20528. Or, you may fax us at 202-282-9207.

Any additional information or copies of the previous minutes of meetings can be found on line at [www.dhs.gov/hsac](http://www.dhs.gov/hsac), and the minutes of this meeting will appear on that web page within 90 days.

Thank you all for attending. The meeting is now adjourned.