Combating Global Terrorism:
Bringing All Elements of National Power to Bear

Darryl R. Williams

February 16, 2006

Lieutenant Colonel Darryl R. Williams, U.S. Air Force, is the director of The Partnership Group, successor organization to the Partnership to Defeat Terrorism (PTDT), part of U.S. Strategic Command's Global Innovation and Strategy Center. The PTDT and The Partnership Group represent a highly successful public-private information sharing architecture that has been aiding the Department of Defense, Strategic Command, and the private sector since November 2001. The Partnership Group partners all elements of national power (e.g., military, diplomatic, private sector, academia, media) into a coordinated front against terrorism and the global mechanisms that support terrorism. Lt. Col. Williams is an internationally recognized expert in terrorism's use of global infrastructures and in global public-private information sharing architectures. He has chaired numerous U.S. efforts investigating and correcting vulnerabilities in U.S. and global infrastructures, both prior to and after the September 11 attack on the World Trade Center. He has a bachelor of science degree in accounting, a master's degree in business administration (international finance), and a master's degree in military arts and strategy.

Oettinger: As you all know, today we are happy and fortunate to have two speakers back to back: Darryl Williams and Gordon Lederman. You have read their formal biographies, so I don't need to introduce them in that sense. One of the interesting features stemming from the coincidence that Gordon couldn't make it in March and Darryl was gracious enough to have him piggyback on his session is that you're going to get a rare complementary display of a couple of approaches to the reform of intelligence. Darryl, who will present first, represents a rather unusual approach: not one that is universally accepted as being the right way to do intelligence. That some people protest that way strikes me as an indication of rigor mortis on their part, but we'll see. Gordon has for the last decade or more been in the business of diagnosing the ills of the older structure and helping to devise ways of reforming it. So these are two ongoing, valid approaches to countering pathologies that numerous reports and commissions have observed in the events of 9/11 and the events regarding weapons of mass destruction in Iraq. Although intelligence failure is a notion that gets bandied about rather loosely, we have in Hurricane Katrina an example of almost laboratory purity of perfect intelligence and terrible operational failure, so the notion that it's always the fault of intelligence is not necessarily a valid one.

So much for anything I should be saying. I'll turn it over to Darryl to tell us what he's been up to. He is happy to field questions as he goes along. This should be more of a conversation than a monologue.

Williams: I'll stand up here so I'm an easier target when you start throwing things. I have three slides that I want to show you. The question you have to answer is: What do these three situations have in common? We have global terrorism (**Figure 1**), which everyone knows about.

Figure 1

Then we have Hurricane Katrina (**Figure 2**), or you could substitute any kind of natural disaster: the tsunami, or the earthquake in San Francisco.

Figure 2

Finally, there's the avian flu (**Figure 3**). It's everywhere. It's in the news today that it's now hit all of Europe. Most of the experts think that we'll probably start seeing our first cases in about nine months, although that doesn't mean it's going to involve human-to-human transfer.

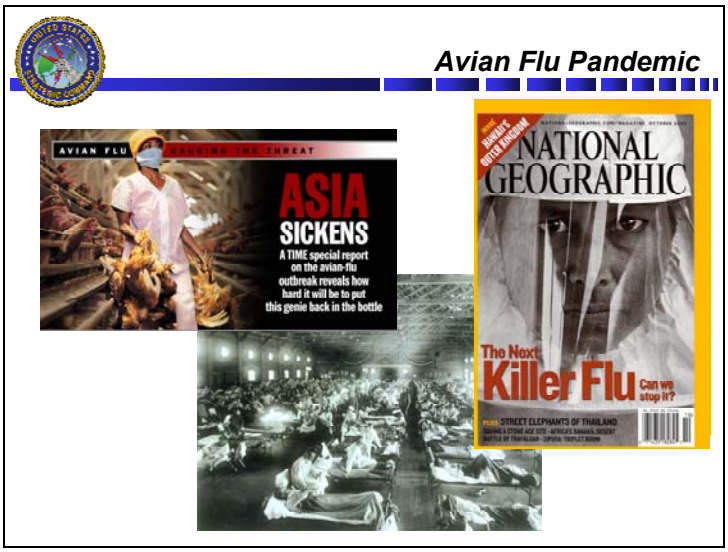

Figure 3

What do those three things have in common? The answer is that each of them affects all elements of power: economic, military, or diplomatic. Then again, dealing with each one of them requires all elements of power. You can't counter global terrorism by saying, "We're going to use a military solution: if we bomb enough people, the terrorists will stop." That just doesn't work. You can't do it with a strictly diplomatic approach, because that doesn't work. There are economic ramifications, diplomatic ramifications, even academic ramifications.

Those were three things to start off with. You actually have a framework. Nowadays no situation has an isolated remedy. You have to look across the spectrum.

That wasn't always the case (**Figure 4**). If you think about historical warfare, when a nation-state would actually invade another nation-state, you could take out the enemy's rail system or ball-bearing plants and you were not too concerned about the collateral effects. They were localized and isolated in a nation-state.

But this is the reality that we live in right now (**Figure 5**): there is no such thing as a nation-state infrastructure that is terrorist related. There is no such thing as Al Qaeda Shipping, or LTTE [Liberation Tigers of Tamil Eelam] Finance, or Abu Sayyaf Logistics. Instead, the terrorists embed themselves in global infrastructures, and I must add that they embed themselves in a legal manner. Now you have a situation where a terrorist cell may be sending money to someone, but is doing it legally through our own global financial infrastructures. The terrorists do that for two reasons. First of all, they want to keep from being detected. When we're talking about a global economic money stream of trillions of dollars, how are you going to pick up a payment of $9,000? Talk about economies of scale and scope! They also do it because they know that if we

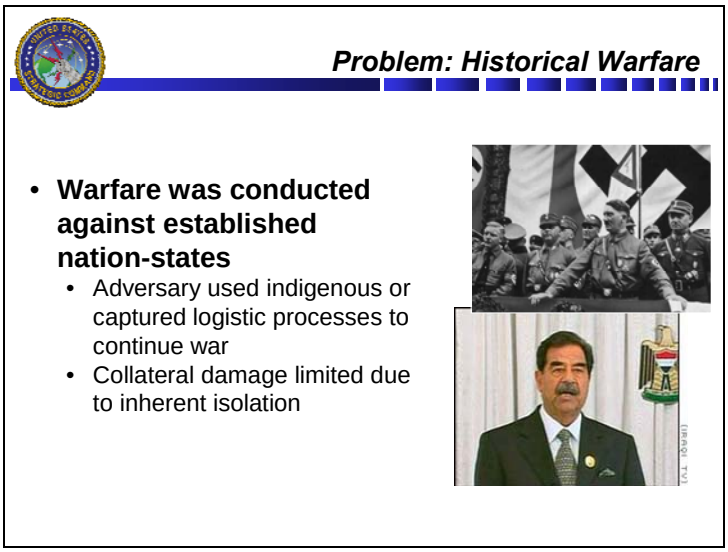

Figure 4

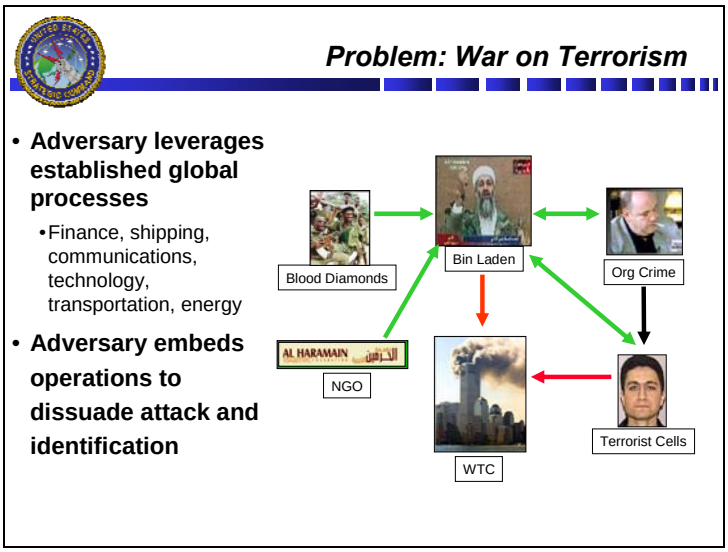

Figure 5

were to try to get them out of that existing stream the collateral effect would be greater than the actual operation we're trying to accomplish. So it protects them and it also masks them.

The slide shows linkages to Bin Laden. It includes organized crime. Any particular transaction could be legitimate. It could be illicit. We don't know. There are charities and blood diamonds, and all that stuff works together.

Let me bring it a little closer to home. You had Atta, who was in Europe, and Bin Laden, who was down in Sudan, Afghanistan, or Saudi Arabia (**Figure 6**). When they sent money over, it

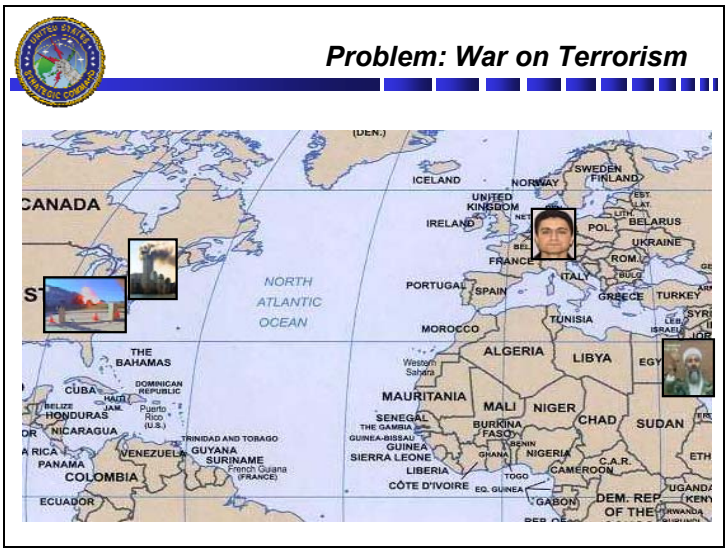

Figure 6

was done legally. The intent was not legal, but the actual movement of money was legal. The movement of people via the airlines to get them over here was legal. The movement of communications was legal, but, of course, the effect ended up being terrorism. The question becomes: "How do you affect these global infrastructures without causing a greater global collateral effect?"

That was the question that came to the Joint Information Operations Center down in San Antonio right after 9/11 (**Figure 7**). In November 2001 the military was asking "How do we affect terrorism without causing a greater global collateral effect?" We can't just see money moving and say, "We're going to shut down the whole monetary process." If we do that all the global economies collapse. But we have a small problem: more than 85 percent of these

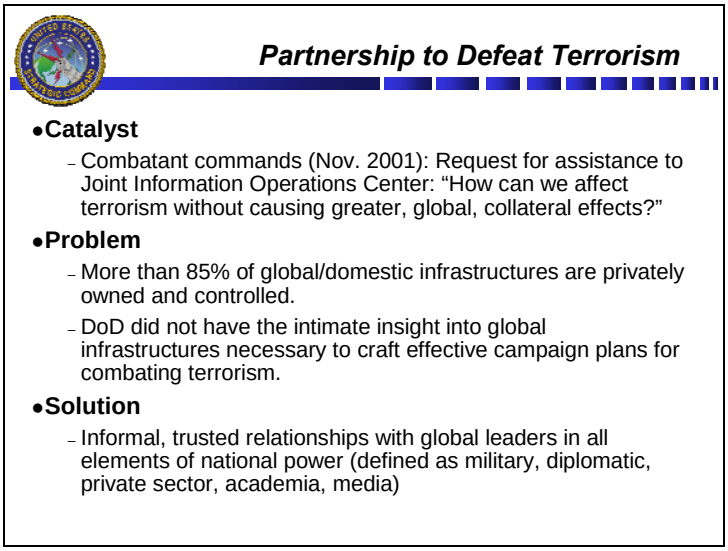

Figure 7

infrastructures are owned by the private sector, so it's not as though the government can say, "We're going to do this, this, and this." The Department of Defense does not have the intimate insight into these global processes that is needed to know what to do. If we see someone moving money through a formal channel, or someone using containerized shipping to move something, we don't have enough insight into that process to figure out the first step toward counteracting a possible terrorist event.

So we started forming trusted informal relationships with global leaders in these infrastructures, and we found that we had tapped an untapped niche. There are not many untapped niches out there, but this was one. It was almost like the Southwest Airlines ad that shows people sitting around a table with a cocktail napkin. I was at a dinner with the head of the Memphis Chamber of Commerce, and at this point we were looking at banking. I was telling him how I wished I knew about banking so that I could help my commanders come up with a course of action. He said, "It's funny that you should bring that up. I just sat down with the vice president of Regents Bank and he was telling me that he wished he had someone to tell about banking, because he's tired of watching the terrorists at work."

In fact, many of these individuals went to the government right after 9/11, because they had lost friends and family in the 9/11 attack and they wanted to help. The government told them just to go back to their homes and sit there and color. At that point, we in government still were not able to amass what they had to give us. The pipe was just too large to get our arms around.

So now we gave them an outlet to help us, and you'll see how they help us. We don't define elements of national power in the same way the government defines it. The Defense Department's definition of elements of power (you might have heard of it) is called DIME: diplomatic, information, military, and economic. Private sector executives think that's the most ludicrous thing they've ever heard, because it doesn't matter whether you're talking about railroads, money, airline travel, or containerized shipping: information is not an element of power, it's a commodity. Whoever has the information has the competitive advantage.

Three individuals won the Nobel Prize in 2001 for devising a new way of looking at economics.[1] When I was in school, we were brought up on the theory of scarcity. If you are the one who can spend enough money to get the information, you have the competitive advantage. These people won the Nobel Prize for saying it's actually the economics of information. It's not a matter of scarcity anymore: it's a matter of so much information coming in that the question becomes how much money you are willing to spend to separate the wheat from the chaff. That is where we're going with this.

Oettinger: The comment I wanted to make goes back to the catalyst of Joint Information Operations Centers and this notion of information warfare. We're not spending much time on that during this semester. In previous years I assigned a rather fat book that deals with that point. Those of you who may be interested in that topic should look at Greg Rattray's book, *Strategic*

[1] George Akerlof, A. Michael Spence, and Joseph Stiglitz, won the 2001 Nobel Prize in Economics for "their analyses of markets with asymmetric information."

Information Warfare,[2] which amplifies to a fare-thee-well the pithy comment that Darryl made with regard to the first three lines of the slide.

Williams: What we found with this niche—and I was never taught this in school—is that once people get to a certain senior level of industry they all tend to sit on each other's boards and they tell each other what they're doing (**Figure 8**). Once word started getting around that there was a conduit for them to contribute to this war on terrorism, the information started moving by word of mouth as they met on these boards. We're down to about two senior-level academic or industry contacts per week. In January 2003 we finally got into the Fortune 500, and once that happened it was trail blazing.

Figure 8

We had to try to capture the potential of what we had. It started out as an information operations/information warfare tool, but once you start bringing in the heads of ConocoPhillips and all these other global corporations your potential eclipses a specific information operations focus. So we try to capture exactly what you have here on the slide.

The bottom line is that we partner with academic and industry leaders to provide options. It's funny, though: the Department of Defense wouldn't execute the options that we would give to them, because the options were a little outside the box—a term that has been used a lot. For example, how do we stop Al Qaeda from launching an attack in the United States? Once we find out what mechanisms Al Qaeda would likely use to launch those attacks, we'll go to senior leaders of the sectors involved. For example, if it's shipping we'll go to a containerized shipper. You'll see how we'll do it a few slides from now. The response to that task may not be what we see here in the U.S. government, with its containerized shipping initiative: "Let's secure the ports." These industry leaders might say, "What you need to do is look in *this* Third World country, because that is a terminal node. If you stop it there, you'll get a ripple effect and you've now stopped the attack." The Defense Department might ask how to solve global warming, and

[2] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001).

these executives might direct them to something that has nothing to do with global warming. So, because they were getting a course of action that didn't fit into their expectations, the Defense Department people wouldn't execute the course of action unless we gave them a way to measure the effectiveness and identified the second- and third-order effects.

So we went back to the industry leaders. What we were basically talking about is corporate risk analysis. "Who is your competition? How do they do things better? If we were to shut down the shipping in the port of Karachi, how else could Al Qaeda obtain those same critical components?" It might be global trucking. It might be global air. Industry is aware of this.

We have to be very strong in filling a critical need, because there are other organizations in the U.S. government that do partnering, and do it quite well. For example, we can talk about the FBI's [Federal Bureau of Investigation's] Infragard.[3] On one job we worked with the Department of Treasury's Office of Foreign Asset Control. However, we found that each one of these government organizations tends to look only at its own particular sector. Treasury might have tremendous partnerships with Citigroup, so they'll go to that partnership and say, "Help us with terror financing." When you know that Citigroup is also a trailblazer in the area of Islamic commerce, you can use Citigroup not just for banking, but also to find out how to gain market access in, let's say, Indonesia. How does hawala work? How do the Sharia laws affect marketing or whatever? You can use them for more than just terror financing, and that's what we do. We go across the spectrum with these leaders, so we bring fidelity to intelligence chatter.

Student: Are you asking people who are in this partnership to do threat analysis for situations that you have identified or the government has identified, or are they doing intelligence collection on potential solutions to problems that have already been identified as threats?

Williams: I would say a little bit of both. There are huge legal concerns, and there are mechanisms in the U.S. government to go out to industry and ask about the data and the threats that they're seeing. We don't replicate those. When we see some of the legal concerns coming up, we don't approach those areas. We try to stay as far away from that cliff as possible.

We will see intelligence chatter, and that chatter will indicate that there is a potential threat somewhere. The chatter may be very broad. What you hear on the news is actually the truth: "We have an impending attack against the United States and it might be …"—whatever. We'll look at that, and the military and the government will look at it, and say, "Okay, let's say that it's *this* target. How would Al Qaeda attack it?" We'll find out that it might be global shipping, or global air, or something else. Then we'll go to industry and ask them process questions.

For example, let's say someone is going to blow up a chemical plant. We would go to the heads of some of the chemical corporations and ask, "What are the vulnerabilities in a chemical plant? If someone were to detonate a bomb, where is the main place where it would take out the entire plant? What safeguards have you put into place? How can they get around those safeguards?" We'll ask them a myriad questions. We get this process information and overlay it

---

[3] "At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States." See http://www.infragard.net/about_us/facts.htm (Accessed on 13 November 2006.)

onto the classified chatter. Now it tends to put a spotlight on the one or two ways where that terrorist organization has to come up with an approach to accomplish its objectives.

Along the same lines, though, you will see in the one example I give that industries, because of their own livelihood, are conducting their own intelligence. They're monitoring their own chat sites to figure out the questions being asked that directly affect their livelihood. So they're a fount of knowledge with no place to give it. Sometimes when we ask them a question, they'll say, "Funny you should ask that. We were seeing *this*…."

Oettinger: Let me try to generalize that a bit and see if you agree. Calling it "intelligence" is, I think, not quite on the mark. One of the reasons for involving the private sector is that unlike the formal intelligence agencies, which are in the intelligence business and therefore are not necessarily knowledgeable about everything that goes on in the world, a bank (for instance) has a strong incentive to know something about the areas in which it works for its daily operations. It's not an intelligence function that is kind of separate from its normal workings, the way the CIA is not in the government business but in the intelligence business. The folks at Citicorp are in the banking business, and because they practice this stuff every day they know what's normal and can detect what is abnormal and treat it as intelligence in a fashion that people walking in from one of fifteen intelligence agencies can't, simply because they don't have the same experience—the day-to-day feeling. That, to me, is one of the most fundamentally important and interesting things about what Darryl is doing.

Williams: Also, the intelligence community has been taking a hit. Some of it may be deserved, but you also have to be aware that technology is rapidly outpacing our ability to analyze the intelligence. With technology today, you can intercept a huge pipe of incoming data in real time. You have a finite number of analysts who can look at that data. So a lot of it relies on keyword searches to help sift out the important stuff, or the intelligence. You do a lot with Google. Bankers, financiers, or shippers all have their own lingo, just as I do in the Department of Defense, but that lingo may not be part of the keyword searches. In those cases the information gets past the analyst, goes on the floor, and is never looked at.

Student: Your process seems to have a problem in that you're finding very good targets for attackers, but you're not necessarily finding very likely targets, because the attackers may not have the same knowledge base as your corporate partners.

Williams: Good point! I thought the same thing, but you will see later on that in essence you're wrong in one way. I'll get ahead of myself with the example and then go back to it. Back when we had the terror alert on Wall Street, the media in Europe were saying the attack was not going to be on Wall Street, it was going to be in Europe. So we started the process, got the information, and found out that the probable target was indeed in Europe. Then we went out to the industry leaders and said, "How can you take down the economy?"

Understand: the adversaries are learning all the time. They attacked buildings. When we talk with the global financiers, they say that we shouldn't focus on buildings. Granted, 9/11 gave us a couple of trillion dollar ripple; however, we were able to reconstitute our economy. What they tell us is, "Don't worry about buildings. They can take out all the buildings they want, but if they take out the leaders you can't reconstitute the economy, because the economy is resident in certain leaders."

My question was exactly the one you raised: “Okay, we know now that you should take out leaders versus taking out buildings, but how is the adversary supposed to know that?” “Well, funny you should ask that. That’s what the chat sites are going over right now. In the chat site that we were monitoring for banking and finance, the question was ‘How do we take out a nation-state economy?’ and the response came back to them, ‘Don’t target the buildings. Target the leaders.’” So that type of dialogue is actually going on in these chat sites, and unfortunately the adversaries are learning.

But you’re right. I went into this thinking, “We’re getting very intimate knowledge on this. Are we giving the adversaries more credit than they deserve?” But when we start talking to these senior leaders we find out that the chat sites are actually giving them this knowledge too.

Student: Your mission statement talks about partnering with global leaders and media experts, and you refer to the head of Citicorp and the heads of the shipping companies. Are these institutional relationships or personal relationships?

Williams: Personal relationships.

Student: So potentially tapping into Citicorp’s market access capabilities would involve digging down within Citicorp?

Williams: If we went that way. We don’t.

Let me back up. The fallacy and the failing of the government—not just the U.S. government—are that we think we can institutionalize trust. We can’t. When things are really boiled down to their basic parts they always come down to a trusted relationship between one individual and another. Where we tend to have problems is when we try to formalize and institutionalize that trust among entities, especially if we institutionalize public-to-private sector relationships, because nine times out of ten we have to start with a formal memorandum of agreement. Now we have to have the legal department look at it, and it always falls apart in the light of formalities. So we characterize this partnership as an ad hoc trusted relationship among people, and you can’t ever discount the people. Once the trust is broken, though, it goes away. It’s very hard to replicate the trust.

Student: What is your relationship with the Department of Homeland Security [DHS]?

Williams: Our relationship with the DHS is very good. The relationship with DHS, Northern Command, and the National Counterterrorism Center is really strange in that we leverage off each other. I work a lot with Jim Caverly at DHS, because he’s in infrastructure.[4] The global leaders with whom I work don’t want to be lumped under DHS, because their business is global versus domestic. For example, ConocoPhillips is concerned about its refineries and drilling platforms in Houston, but it’s just as concerned about Nigeria, Venezuela, and the Caspian Sea. So they like this particular partnership, because we look at things in the global versus the domestic realm.

Now, the majority of our taskings are classified. They may be classified because of sources and methods, or they may be classified because, as was already indicated, they might identify a vulnerability. When we go out to industry—and you’ll see how we do that—it is unclassified and

[4] Jim Caverly is the director of the Infrastructure Coordination Division, Information Analysis and. Infrastructure Protection, DHS.

virtual. Once the information comes back and we fuse it with other information, it starts becoming classified again. The government agencies like that. If we see that the path that industry is giving us is a homeland security issue, DHS is right with us, as are the FBI and all the other organizations. Basically they're leveraging off this, but they're still trying to construct their infrastructure protection matrix and everything else. This is a way of getting momentum while the government agencies try to formalize an institution.

Student: What is the incentive for these corporations to join this partnership? I understand the government's getting something from it.

Williams: That's a great question. The incentive is twofold. The first incentive that brought them into the fold was patriotism. There's no way around it: these people are patriots. Granted, they make billions of dollars, but they're patriots. When you sit across from them in their homes, they have pictures of their grandchildren right behind them.

What keeps them in are actually two things. First of all, we don't badger them. You'll see later on that as we create the access we'll build the trusted relationship, but we may not contact them for a year or two. It's more like *Mission Impossible*: the task will indicate that this is the right person to answer a particular question.

The other thing that keeps them in is their livelihood. They're not just afraid of another 9/11 type of attack; I would argue that they're more concerned about a government response to a 9/11 attack. If a container goes off in New York we'll probably shut down all our harbors until we can figure out what to do. Now you have three weeks before you see tremendous economic damage, which starts rippling through rail, trucking, consumers, everything. If these leaders can give us a way of restarting the economy, or restarting the shipping, it's to their benefit to do that. So we give them a voice. Patriotism brings them in; livelihood keeps them.

Also, when we ask them a question, you'll see that it's virtual. It takes about fifteen minutes, and that's it. We're not telling them "You need to come to Omaha. We'll do a roundtable, stay for three days, and rap a little bit." Instead, we get the task from whomever. We pick a particular leader and we get him on the phone within a sixty-minute benchmark. We tell him what we need, he gives us the information, everything is shut off, and he goes on his merry way. So for fifteen minutes he gets his voice heard, which may aid us as we go along.

I do have to continue to foot-stomp on this area. We bring fidelity to intelligence chatter, and we support development of counterterrorism actions. We're not a Tom Clancy Net Center. We don't do operations. To use a private sector analogy, we are a brokerage house. People come to us with a need, we broker the person who has a need with a person who has a solution, and then we step out of the way.

You may think it's simplistic, and that surely someone must be doing it. No one is. When it was in its infancy we tried to give this program to everyone from the DHS to the National Security Council, and no one would take it. It was almost like a leper colony when we dealt with government-to-private sector relationships. Now that it has this network everyone wants it, but no one knows how to maintain it. We briefed this to Secretary Rumsfeld a couple of times. He said, "Okay, Strategic Command, you keep it, because you already have the trust, but you also have the global mission for weapons of mass destruction and Global Strike." So we have it still.

We do deal with the tactical and operational levels of war (**Figure 9**). However, with the avian flu task we're really getting into strategic issues, and that task came from the Centers for Disease Control [CDC]. They heard about what we're doing. They needed access to global absentee data, because they figured that if they could get absentee data it would give them maybe a two- or three-day jump on formal government reporting of a flu outbreak. The reason is that a lot of people are like me: when I get sick I don't just run to the hospital. I try to get some over-the-counter drugs and self-medicate until I'm so sick that I have to go to the hospital. The problem with avian flu is that you have about twenty-four hours and then you die. So they have to know very quickly when the outbreak is starting. Before, a three-day head start didn't matter, but with H5N1, the avian flu, every day counts.

Figure 9

So the CDC came to us and said, "Can you broker your contacts in the global airlines?" What we're doing right now is brokering a contact with the Star Alliance, which has sixteen global airlines, from Lufthansa to United Airlines. Will they get the data? Maybe or maybe not, but at least we're putting them in contact with the people who can help.

We have access to far more than a thousand global leaders, but what with mergers, acquisitions, hires, and fires, a thousand is what we publish. It was vetted through the secretary of defense and all the intelligence agencies. It was briefed to the president twice. Remarkably, the first person we briefed was not Rumsfeld; it was actually Secretary Ridge at the DHS. We've taken some CEOs [chief executive officers] and CTOs [chief technology officers] over to England on two or three occasions to talk to the British interagency groups. We've been to Singapore and a few other places.

As for the keys to success, I've already touched on trust, unclassified, and virtual. Don't underestimate the virtual. I don't know if any of you have read Thomas Friedman's book *The*

World Is Flat.[5] I would argue that the world is not flat. Flat indicates that there is a length to the world. There is none. The world is actually a dot.

For example, the way we do planning in the Department of Defense is that we send out an invitation and bring everyone around the table. We sit down and we accomplish planning over a week, and then the plan goes out for people to critique it, kill it, or whatever. The way it's done in the real world is virtual. I was given a task over the New Year's holiday to come up with a concept of operations for this. The way we worked it was that I had a CEO who blew out his knee on the slopes of Vail, so he was sitting in his suite in Vail with a Blackberry. We were talking that way. We had another CEO in Delaware with a laptop, another one was actually up here at Harvard, and we were all passing files, holding net meetings, and at the end of twenty-four hours we had an airtight concept of operations. That's how the world works. It's got to be virtual.

The Partnership to Defeat Terrorism architecture is a horizontal collaboration network (**Figure 10**). If you always keep in mind that we're brokering the person with the need with the person who has the information, the most difficult part is finding the person who has the information. There is an expert on anything, from the mating patterns of the sponge to global commerce. How do you find that person?

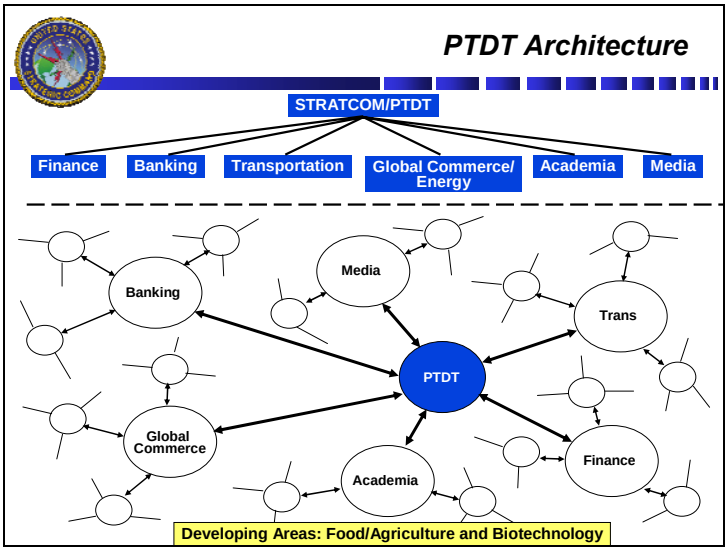

Figure 10

We've broken the infrastructure into sectors. Here I just show six notional ones. We'll have two or three of the globally recognized leaders of each sector. If we know to whom we should go, because of a trusted relationship that we've already built, we'll go directly to that person. If we don't know whom to call we'll go to one of our cutouts. It's their job to know the mergers, firings, and hirings, and they'll say, "You need to talk with *this* individual in *this* corporation. Let me make the call for you and establish the trust." That's how it works.

[5] Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-First Century* (New York: Farrar, Straus and Giroux, 2005).

We energize sectors. They go out and find the individual for us. In the case of academia, we had to come up with a particular individual for a very specialized area of study, so we called our cutout in academia and said, "We need an expert in this particular field," and he found an expert in Idaho. That's how it works. It's very fast.

Bieda: You say that you initially call to form the trusted relationships, but that the word also spreads. Do you have an idea what proportion of your more than a thousand trusted relationships actually came about from people's calling you and saying "I want to be called"?

Williams: We get called a lot, and that's why Jessica Meyeraan[6] and I were on the road quite a lot. You can do a lot of things virtually, but that trust has to be cemented through personal interaction, so we spend about three weeks out of a month on the road.

Student: Would you say a majority of your current count called in?

Williams: The majority of the count at this point results from a spreading of the network on its own. I would say about 150 to maybe 200 are actually people we contacted.

As it said on the previous slide, access does not mean that we talk to these individuals on a daily, weekly, monthly, or even yearly basis. What it means is that we have sat down with them on a one-to-one basis and told them what we do, and they volunteered if they wanted to give us access. Access means that we have a telephone number specifically with them so that when we get tasked we dial this number, it comes up on their pager or cell phone, they realize who it is, they excuse themselves from whatever they're doing, they get on the phone, and we talk. We try to keep the time from when we get a task to the time when we have that leader on the phone to around sixty minutes. Sometimes we're within fifteen minutes, sometimes it's a couple of hours, but it never goes much longer than a couple of hours.

Right now we're trying to get into the agriculture and biotechnology areas.

Student: You mentioned Idaho and Vail, so I assume you're talking about American leaders of global industries. In *The World Is Flat* doesn't Tom Friedman say that that the future of networks like this is global and that dealing with the leaders in Pakistan and Indonesia is a natural next step?

Williams: That's a very good point. It's not that we haven't been approached by truly foreign corporations, it's that we have to walk before we run. This thing has only been going since 2001. What we have done is focus on global corporations that are headquartered in the United States. The reason is that initially we had a big stick: the Foreign Corrupt Practices Act. When we go over to England and meet with their senior leaders, they're trying to build a similar node with British industries that are global, because there are legal considerations they have to work with in their nation-state infrastructure.

Although we've been approached by global corporations, we haven't branched out past the United States because we haven't needed to. The only sector where we may need to go outside is containerized shipping, because the four major containerized shippers are not headquartered in the United States. However, we've been able to handle any containerized shipping problem by working with U.S. shippers. You might have read a book by Steve Flynn, *America the*

[6] Lt. Col. Jessica Meyeraan is director of operations, The Partnership Group.

Vulnerable.[7] He's been part of our group for quite a while, and a globalized shipper from Hong Kong, John Meredith, who heads Hutchison Port Holdings, has offered to help, but because he is a foreign entity we have not approached him. We haven't had to. As we get to the necessary evolution we will have to start bringing in the foreign corporate world. Right now the Department of Defense would not deal with that.

Student: You said that you and Jessica are traveling around a lot meeting people. Is the goal redundancy, so that they have personal relationships with two people in your group rather than just one, in case you depart or something?

Williams: That would be optimal, but it's not efficient. This is actually the first time that we have traveled together. Usually we're covering different ends of the spectrum. For example, when I was in Hollywood she was in Atlanta working with the CDC, so we have to separate.

Our mantra is not redundancy, it is leveraging. We will not duplicate any other kind of organization. If we know that the DHS is doing something better than we can do it we contact them and find out ways that we can help them. We will not duplicate what they are doing.

Student: Do you have any transition planning at the moment? Presumably, you do not want to do this forever.

Williams: Right, and you'll see where we're going. The transition planning really took place at the insistence of the private sector, which is unique when you think about it. Most of the time it's the government that comes to the private sector and says "Help us." This time the private sector looked at the PTDT, just as you did, and said, "There's no longevity in this. If someone meets the front end of a truck, that node is shut down." So they are the ones who are pushing for an architectural change.

Student: Could you go into a little more depth on the role of academia? When you first mentioned it, I made the assumption that academia had a different role inside each of the broader categories—for instance, in transportation or in finance—but when the last schematic (Figure 10) was shown it seemed that academia was a separate entity.

Williams: It is. Academia is actually a fount of knowledge. A lot of times we'll go into a meeting with preconceived notions and all those notions are destroyed. For example, we went to a meeting with media executives and asked "If we come to you, can you give us ground truth about what's happening in a hot spot? For example, do you have embedded reporters in Kabul? Can you help us with that?" They said, "If you're looking to us for ground truth, then you're crazy!" That was news to us, because we spend a lot of money on media analysis. They said, "You have to understand the process. After the reporter gets the story it goes to the editors and goes through a scrubbing, then it goes through a publisher, so by the time you get the story it's only snippets of reality. If you want to know what's going on in a country, go to academia, because wherever there's a hot spot there's embedded academe." We found that to be true. I talked to some troops who had just came back from Iraq. Most of the reporters stay in the Green Zone and wait for sources to come to them. Most of those sources are in academia. We use academia quite a lot.

---

[7] Stephen Flynn, *America the Vulnerable: How Our Government Is Failing to Protect Us From Terrorism* (New York: HarperCollins, 2004).

Also, as administrations change the people out of power usually go into academia, waiting for the administration to change again, and then they swap out again. It seems like a revolving door. So academia is a tremendous place for policy. In fact, my first visit to academia was actually at Harvard with Elaine Kamarck.[8] She was a fount of knowledge. She worked on reinventing government.

Oettinger: She's a good example, because she was an official of the Clinton administration.

Williams: We went to her with a slide of how we were going to set up this partnership to beat terrorism. She said, "If you do that, you're going to be in jail. You really want to do it *this* way." We listen to stuff like that.

Also, we might find that the particular expert may not be in corporate America. He or she might be retired, or be teaching. For example, we needed information about the exchange system of a very small country: how does the exchange system work for stocks and the movement of all its assets? That individual had retired and is teaching at Southern Methodist University.

Academia is critical, and we do not discriminate against particular institutions. We go as eagerly to the small institutions as we do to the larger ones. We don't care too much about their religious affiliation. We'll go to the Catholic University of America and we'll go to an evangelical Baptist university, because each has a niche. You just never know when that niche is going to come up.

When we briefed the secretary of defense he was having a small problem with the Total Information Awareness program that Admiral Poindexter was leading. It was designed to do Web crawling: pull information from the Web, maintain a database in the U.S. government, and then use that database to find bits and pieces of nuggets without really having much privacy oversight and so on and so forth. That hit the media airwaves and Secretary Rumsfeld was feeling those ripples. He used very colorful language to make it clear that he did not want to replicate the Total Information Awareness program. By the way, he probably only heard this briefing because we took three CEOs with us, and since he was also a CEO we got instant access and it went well.

We took six months and researched the partnering process. We interviewed everyone, from failed to successful. An example of successful is NSTAC: the National Security Telecommunications Advisory Committee. That's a good public-private partnership. We sat down with John Koskinen, who was the Y2K czar. We sat down with a lot of people who ran the Information Sharing and Analysis Centers.

This seems to be the sum total of the areas that will bite you when you do public-private partnering (**Figure 11**). There might be more, but these are the big ones. Any time the public sector maintains a database you're asking for trouble. Even if you have all these safeguards, you're asking for trouble, because we also live in a world that goes by perception.

---

[8] Elaine C. Kamarck is a lecturer in public policy at Harvard's John F. Kennedy School of Government. She served in the White House from 1993 to 1997, where she created and managed the Clinton Administration's National Performance Review, also known as "reinventing government."

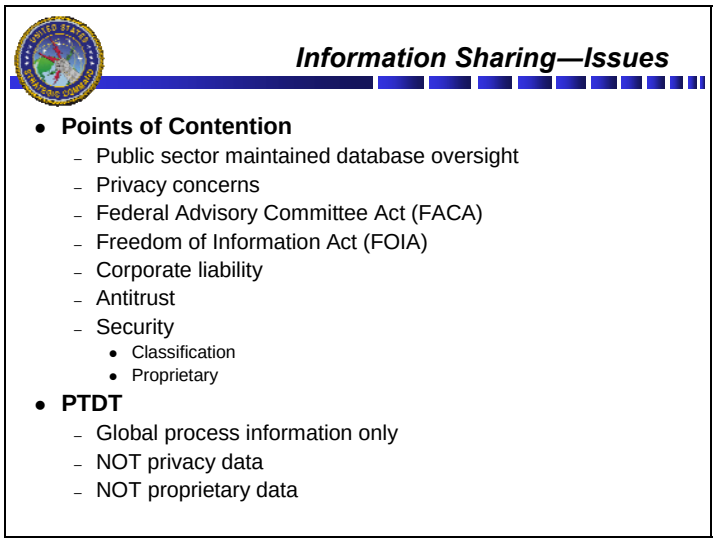

Figure 11

Privacy concerns and the Federal Advisory Committee Act [FACA] are where Vice President Cheney ran into problems with his energy commission.[9] Whenever the private sector gets together, forms consensus, and gives that consensus to the U.S. government, it could be running against FACA. Other potential problem areas are the Freedom of Information Act [FOIA], corporate liability, antitrust rules, and even security, from proprietary information to other security. As of now we have not had to worry about this, because we don't deal with that type of information. We deal in global process information only.

This does not mean that the private sector has not approached us and asked us if we wanted data. For example, when we briefed Secretary Rumsfeld one of the people with me was Randy Lerner, who not only owns the Cleveland Browns but also owned MBNA Corporation, which issues credit cards. I think they were just bought out by Bank of America. He told the secretary of defense, "We have taxonomies set up in our systems to detect fraud. For example, we know that if someone steals a credit card, the first thing that person is going to do is go to a gas station and see if that credit card works. He will probably charge about five dollars. From there he'll go to an electronics store and charge hundreds of dollars." So I had one of my staff down in San Antonio who wanted to buy a DVD recorder go to a gas station first. Sure enough, he went to the gas station and then he went to Radio Shack, and fifteen minutes later his phone was ringing and MBNA was saying, "We want to make sure these charges are yours." Randy Lerner told the secretary of defense, "When it comes to chem-bio weapons, if we know that someone routinely charges electronics gear, electronics gear, and electronics gear, and then all of a sudden charges a ton of fertilizer, diesel fuel, and a U-Haul truck, that comes up as a taxonomy of a possible matrix to build a fertilizer bomb. If you give us terrorist taxonomies, we can inform people that we've got a problem." According to Randy Lerner's counsel, as long as they give information that meets a terrorist profile they are somewhat absolved from corporate liability. I don't know how that

[9] The Federal Advisory Committee Act was enacted in 1972 to ensure that advice given to the executive branch by advisory committees, task forces, boards, and commissions was both objective and accessible to the public.

works. I am not a lawyer. We deal with global process data only, period. So don't go out and put on your blog that PTDT invades privacy. We don't!

What is that process? It's how they do business from point A to point B. If we know that the adversary is about to target someone overseas, we want to know what that adversary has to do to get that target. We'll go to the global shippers, global financiers, global whatever, and ask "How do you do business from point A to point B?" To them it's very boring information. They live that every single day. But to us, when we overlay it onto classified chatter, it usually puts intent to what the adversary is trying to do.

Oettinger: I think there is another important element that you may get to, but that strikes me as vital. Everything is relatively easy given a profile that is equivalent to keywords with which to go into a database. What your system provides is the potential for these executives to create something that is not part of the profile, because either they have experienced it and nobody in the government has, or because, given the nature of your queries, it occurs to them on the spur of the moment that a particular event or activity that is not in the normal course of business might happen. Computer search programs don't have creative ideas like that. So there is that element: these sentient, intelligent human beings are engaged in extensive activities about which they have knowledge, so they can not only detect problems but also think of anomalies and alternatives in a way that the best-known software cannot.

Student: My hair stood on end when you said that as a result of this partnership MBNA may identify someone with an MBNA credit card who buys a U-Haul and fertilizer as a terrorist.

Williams: They don't. The MBNA chairman of the board was telling the secretary of defense that he could use these taxonomies to help the U.S. government. That is not a given.

Student: If a Yahoo executive were to say "If you search for 'U-Haul' and 'fertilizer' we may be able to provide the federal government with that kind of information" it would cause outrage about privacy issues. As a result of the partnerships that you facilitate between the government and the private sector you might raise this whole other privacy issue.

Williams: No, because we do not deal with anything that is privacy related (or proprietary, for that matter). We don't ask Coca Cola for their secret formula or anything else. We don't ask FedEx how they do shipping faster. That does not mean that there aren't good public-private partnerships out there with other entities, but they exist under evidential criteria and law enforcement criteria with subpoenas and everything else. You cannot skirt the law. The law is there for a purpose. We just deal with process.

Oettinger: You've just opened up a big topic. Much of the legality or illegality of certain acts depends on who, where, under what circumstances, in which industry, and so forth. Crudely, in the realm we are dealing with, law enforcement and intelligence operate under very different legal structures. There are some overlaps, but something that is okay in law enforcement may or may not be okay in intelligence. In spite of what you see in the newspapers, counsel in most of these agencies are intensely aware (as you can hear Darryl is) of the need to stay within the law. That doesn't mean that occasionally somebody stupidly or roguishly doesn't do something bad, but the concern that you hear here is a pervasive one. In fact, a citizen needs to be concerned about whether the converse—the perversion of that good intention—leads to ass-covering and inaction, so that for fear of the law you bend over backwards and do nothing because it's safer than doing something. That, under certain circumstances, leads to the "How come you failed to connect the

dots?" kind of thing. How the civil servant is treated depends on the mood of the public. You always want to think of these two extremes: roguishly or stupidly doing something illegal, or, on the other hand, self-protection, doing the safe thing, which is always doing nothing, because nobody can put you in jail for doing nothing.

Student: You say you've been operating for five years, and you've had your tendrils in the Fortune 500 for three years. Can you give us a sense of how many incidents of terrorism in the United States you think you've averted?

Williams: Remember, we deal on a global level, so I can only tell you that we've used this over thirty times. What I mean by "using" is that we have received a specific task, based either on conjecture—someone sitting in a think tank asking "What if…?"—or on actual classified chatter. We have received a tasking to bring fidelity to that chatter more than thirty times.

Student: Of those thirty, how many do you think were research and how many were truly operational?

Williams: I'd rather not go into that. Just leave it at thirty.

Student: You mentioned that the initial motivation for a lot of these industry leaders was that they had information that they felt they needed to communicate to the government, but your talk has primarily focused on your receiving tasks and then reaching out. Is there any inward flow of unsolicited information that results in some action being taken by your group ?

Williams: From the private sector, no. We actually discourage that. There are mechanisms for the private sector to pass that information and we would not skirt those mechanisms. Whether they are efficient or working well is to me irrelevant. The private sector has to stay within the bounds of the law. If they were to come to me and say "We've heard something" I would refer them to the FBI.

Also, I've sat in some board meetings where they say, "Okay, we'll give you this information, but we expect you to give us threat information." We terminate the discussions at that point, because there is a mechanism created to pass threat information to the private sector. They may say, "We don't like it. It's inefficient. We don't get it," but to me that's again irrelevant. As an American I want it to be as fast and as efficient as possible, but I'm bounded by certain laws and limits. That's all I can do.

Oettinger: I can't overemphasize the point he's just made, because again, from the viewpoint of national security as opposed to control of rogue government agencies, that could be regarded as a deficiency in the structure. Jim Bieda is looking into some of those things and in one of our forthcoming sessions we will go into that question in greater depth. The central point that I think you should carry away from this phase of Darryl's presentation is that the structure of law—not only statutory or common law as enacted by Congress, but also executive orders, traditions, organizational culture, and so on—figures into what a given agency thinks it can or cannot, or should or should not, do, and that gets to be a very complicated mess. It's one of the reasons why, when we turn to Gordon [Lederman], you will see that reform of the intelligence community is such a difficult task. You're dealing with multiple agencies whose cultures and structures under the law, et cetera, differ wildly for reasons good and bad.

Bieda: I'd like to add something to Darryl's comment about the credit card industry's wanting to give that data to him or to the secretary of defense. Keep in mind that corporations can do

anything they want with your data. They have a privacy policy that they will put out to you, but they can choose to police the data that they use for internal business in any way they want to. The question for them is how much they want to spend to mitigate a certain risk.

Williams: This is one of few unclassified examples that I can give you of the use of the PTDT (**Figure 12**). Professor Oettinger saw the classified briefing that we show to senior leaders in the government, which actually walks step by step through examples of where this was used. Understand as we go through this that the PTDT has to be unclassified, it has to be virtual, and it has to rest on trusted relationships. That's what sustains the bedrock. This happened back in August 2004. We had intelligence chatter. Usually CNN [Cable News Network] is a great place for us to find unclassified transcripts to take to the CEOs. So on the left of the slide we have the intelligence chatter. We have Bin Laden's goals: affect elections, collapse the U.S. economy, fracture the coalition. On this basis we raised the terror alert on Wall Street, focused on the Prudential Building, and focused on Washington, D.C. I'm sure many of you remember this.

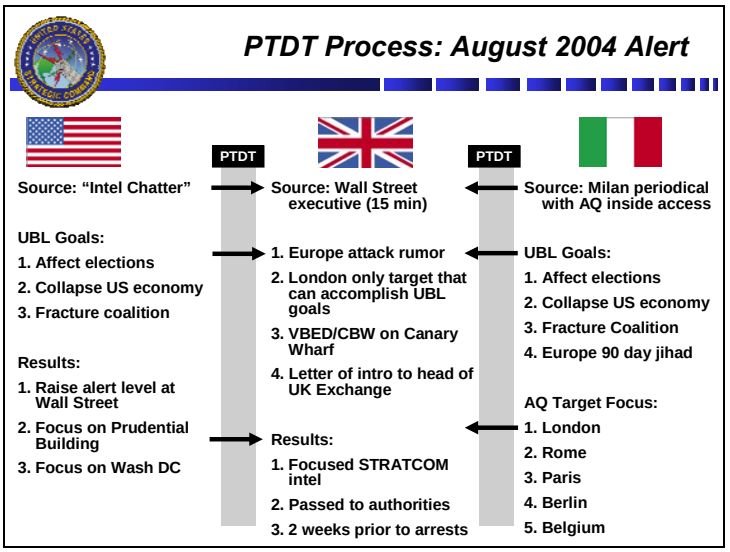

Figure 12

At the same time, we had an analyst in Strategic Command who was reading a periodical from Milan, and it seemed that for some reason a particular journalist had the inside track on Al Qaeda. Maybe he just guessed right or whatever, but his last few predictions were right on. The Milan periodical was stating that it was not going to be an attack in the United States, it was going to be an attack in Europe, because of the end of a ninety-day jihad. The journalist's sources were telling him that the focus was going to be on one of the five areas in Europe listed at the right.

So we had a conflict. How would we resolve this conflict? At that point we were asked to go out and energize the partnership system to see if we could get a resolution. It was like *Mission Impossible*. We went through the Rolodex to see who the right person was. In this case the person was a vice chairman of Bear Stearns. He is the globally recognized leader not only in U.S. exchange systems, but also in all exchange systems. As the World Trade Center was collapsing

this individual was convening a board of financiers in New York to make sure that everything continued to run.

So I called his number and within fifteen minutes he was on the phone. All I did was read both transcripts to him. Remember, the discussion has to be unclassified. Also, you have to look at operational security [OPSEC], which is a big factor. You don't want to go out to an Indonesian shipper the day before you're going to conduct an Indonesian operation. You can say something that is unclassified by itself, but when you put it together with everything else that is going on—say, pizza deliveries at the Pentagon or something like that—you now know something's about to happen. So we have intelligence oversight on these things, we have OPSEC oversight, and we have legal oversight to make sure we stay away from the cliff.

We read him both transcripts and asked him, "What do you think?" He said, "It's funny that you should ask that, because we've been monitoring our chat sites and everything is pointing to a European attack. So we're not even gearing up for a U.S. attack, we're gearing up for a European attack." He was the one who had given me the information that terrorists want to take out leaders versus buildings. With that in mind, and knowing Al Qaeda's goals, we looked at these five areas in Europe and came up with the best place for them to accomplish the goals. He said, "You're down to Belgium and London. I just left the office of the Belgian ambassador and they're plugging up the holes that I'm telling you about. So it's got to be London." Then he said, "If I were to do it, knowing that the Exchange just moved to a new location and knowing that the leaders were there, I would use a vehicle-borne explosive or a chem-bio weapon on Canary Wharf. Just in case this happens, let me broker you to the head of the UK [United Kingdom] exchange system." We talked for maybe fifteen minutes, he hung up, and he went his merry way.

Then I went out to try to find corroborating intelligence. Understand that if you do not have this framework a lot of times the intelligence apparatus is a glorified game of Go Fish. You basically sit there with your cards and ask, "Do you have a two?" "No, go fish." "Do you have a six?" "No, go fish." When we get the insight from industry we go back into the intelligence apparatus and ask, "Do you have this?" "Yes, we do. It's right here." The U.S. intelligence apparatus, and most government intelligence apparatuses, were specifically designed for forensics. "Something happened, what did we miss?" You really need insight—human source intelligence [HUMINT], and our HUMINT has been pretty much done away with—to give you a pointer. "Did you look here?" At that point we found that there was an Al Qaeda cell in London.

We've been over talking with the UK on numerous occasions. We've shown them this slide, and we've told them categorically that this did not lead to the arrests. They were well aware of that cell. But what it did for us in the United States was that when we brought all the elements of national power together we were able to determine that the cell existed, even though we had not heard about it from them.

All this was accomplished two weeks prior to the arrests. We guessed the mechanism wrong. The Queen said before Parliament that the target was Canary Wharf; however, she also mentioned that they were going to hijack two airliners. One was going to crash into Heathrow, and one was going to crash into Canary Wharf. So you miss some things. This is one of the more mundane examples. Some of the other examples were pretty good.

We're getting toward the end (**Figure 13**). In San Antonio the secretary of defense tasked Strategic Command to oversee this, so we moved it from San Antonio up to Omaha. There we formed partnerships with the Peter Kiewit Institute. The Peter Kiewit Institute is a technology institution probably second to none. It's what you get when you have a couple of billionaires who don't want to be second. Whenever they find another organization that has better coursework than they do they go out and hire all the professors, so it is a tremendous computer center. We wanted to create a network much like the Bangalore call centers mentioned in Tom Friedman's book, so we could sit there and actually pull up CEOs from all around the United States and talk to them and get collaboration.

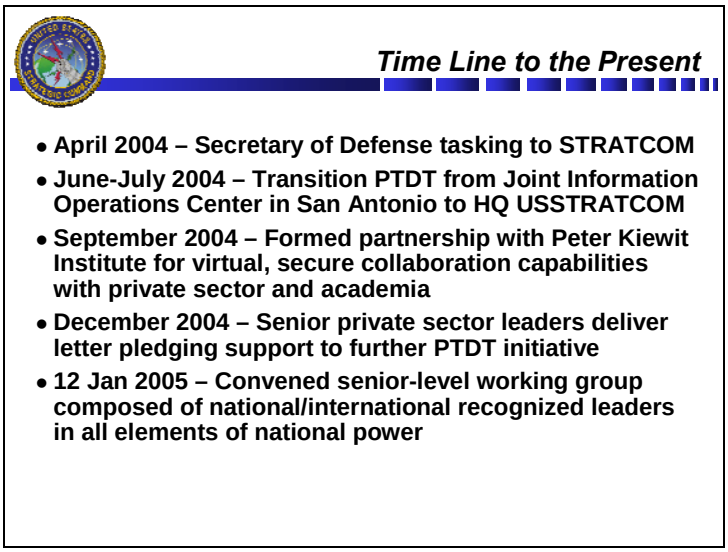

Figure 13

Then something unusual happened. A group of private sector leaders got together around the December timeframe and sent a personal letter to my commander and our four-star, General Cartwright, saying that the system had no longevity. If one person dies, the network collapses. If he would spearhead a formalization of this process, they would throw their weight and credibility behind it.

So we called their bluff. We said, "Okay, come to Omaha." It was January 12, and it was almost an apocalyptic day in Omaha, Nebraska, with snow, sleet, rain, hail, or whatever. We had everyone from Strategic Command, Northern Command, senators, state, industry, and the UK, and we sat around the table (**Figure 14**). We came up with findings (**Figure 15**). These findings were nothing new: the adversary doesn't have an established infrastructure; the only way to attack terrorism is through a synchronized mechanism using all elements of national power; there must be a center that formalizes this; and they—meaning the private sector—have to have a part in manning it.

Figure 14

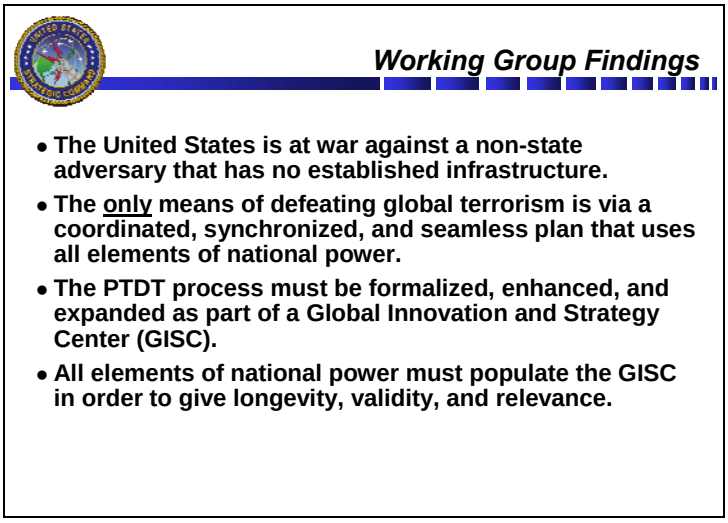

Figure 15

Oettinger: It's an interesting thought that may lead to a term paper for somebody, but that particular concept is reminiscent of centers involving coalition allies. Imagine, for example, Joint Forces Command in Norfolk, Virginia, and a place where there is an intelligence or a planning cell that's strictly United States, and in another room there are some UK people and some others, and you're trying to do something without having them in direct communication. Why do I think of that as an example? Going back to Darryl's and Jim's point about different legal permissions, can you mix industry people whose handling of data falls under one set of rules with government people whose handling follows another rule? Perhaps under present laws they may be in the same building, but I'd be curious if you can elaborate on how you're going to get them to collaborate with greater efficiency than "through a glass darkly," as has been the past experience with some of these efforts.

Williams: We're not there. We're at about a 20 percent solution. Right now we deal with a zero percent rate, so 20 percent is pretty good.

Oettinger: I can't resist telling a personal anecdote on that score. A number of years ago I was consulting for the President's Foreign Intelligence Advisory Board, and the chairman sent me over to the Pentagon to talk to the chairman of the Joint Chiefs about something or other. The colonel who was his gatekeeper threw me out. As he threw me out, his words were, "We don't need you intelligence weenies mixing yourselves up in operations." So I reported that back to headquarters and that was the end of it. That gatekeeper became a four-star general and was the supreme allied commander in Europe during the Kosovo exercises. This was General Joulwan, and he became an apostle of intelligence sharing. Why? Because his people were in the trenches there with Russians and Yugoslavs, et cetera, being shot at by they knew not whom, and so it became imperative to share intelligence in a fashion that had not been tried before. Under fire, folks are more likely to share than not, and under the right circumstances this guy who at one point vehemently did not want to have intelligence mixed up with operations suddenly became an apostle of the close collaboration between operations and intelligence. So things can change, but it's important to spot the changes when you see them. As Darryl said earlier about all the legal constraints, things suddenly pop up, and to my mind that's one of them. I may be wrong and you'll prove me wrong.

Williams: Understanding that we always stay as far away from the cliff as possible, the first thing we thought of as we sat around at this meeting with these industry leaders was "Why don't they donate people to this center?" But then we'd have private sector people sitting in the building. What would happen if all the private sector people got together and formed a consensus and came to the Department of Defense and said, "You need to do *this*"? That would go against FACA. Would we be able to beat it? Probably, but I don't even want to go there.

So then it came down to "Why don't we in the U.S. government hire those people and have them in the center? We'll pay for them, so they'll be there at our expense." Then we would have private sector people employed by the government, so any of the information that they get would possibly fall under FOIA. Could we beat that? Probably, because of national security, but we would still have a problem.

What we identified as the solution were entities called FFRDCs: Federally Funded Research and Development Centers. Since they are not for profit, if we give them the money and then they hire the private sector entities, those people become FFRDC employees, they're absolved from both FACA and FOIA, and they can actually function in both worlds. That is the mechanism we're using right now to help us with that.

Oettinger: There is in that simple remark a whole area of inquiry that is of enormous importance. People use the terms "public" and "private" very glibly, as if they were poles apart. There is in fact a continuum. If you think about it, it includes things such as FFRDCs, authorities such as MASSPORT [Massachusetts Port Authority], entities that have the full faith and credit of the government behind them, and entities that have their own financing but would not be bailed out by the government.

In spite of all the nasty jokes about lawyers, creative lawyers are a thing of joy and beauty and are absolutely essential in getting stuff like this working, because otherwise our obvious

solution is to do nothing so we can stay out of jail. So don't fall prey to the prevalent habit of sneering at lawyers. They're as important a set of experts as anybody else.

Williams: This is the Global Innovation Strategy Center (**Figure 16**). We just moved into it this month. It is a world-class facility (**Figure 17**). It does not just face global issues, it faces the hard problems.

Figure 16

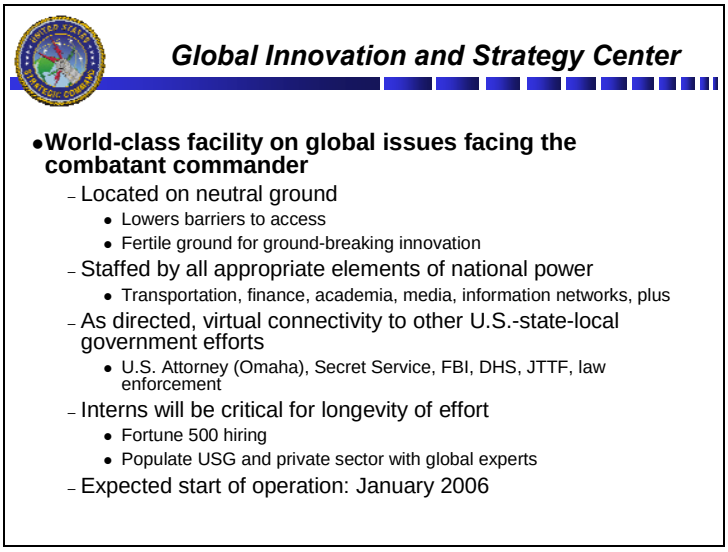

Figure 17

Because pride is a huge motivator in the U.S. government and in the Department of Defense, by the time we get a problem it has usually been looked at in fifty or sixty different ways. They come to us as a last resort. What we do is apply all the elements of national power against it.

A question came up earlier about trust: is it individual or is it institutionalized? After working with the private sector these individuals from the FFRDC will be blessed with access. Right now we have FFRDCs that look at five areas: media, maritime transportation, finance, academia, and the information networks. The individuals in the FFRDC will not be given access to the leader per se, but the leader will give them a point of contact in his organization, such as his executive assistant. Jessica and I still have to go out and broker the initial trust, but after we do that we'll arrange another meeting to transfer that trust to this individual who will act as the sector liaison. It's not the optimum solution, but it's the best we can do, and if we're going to have longevity it will give us at least a 20 percent solution. It will be up to those particular sector subject matter experts to make sure they're monitoring acquisitions, mergers, and so on.

Student: Do you consider the employees here more like analysts or more like contacts?

Williams: Brokers is the proper word. In fact, the CEOs call them librarians, which is a strange title, but they say, in essence, "If I have a problem, I go to the Library of Congress. Suppose there's a chem-bio factory that just got a load of fertilizer or nitrates of some kind. Whom do I call? This guy looks at his Rolodex, goes to his card catalogue, and says, 'I need to call *this* guy.'" So they look at them as librarians. It's not a very sexy term. I like "brokers" better.

People have a need, and, as directed, we are connecting with other U.S. state and local entities. A U.S. attorney in Omaha is a big fan of this. The Secret Service has some interesting things going on right now. So does the FBI.

Interns are critical. Our intern program started, I think, on January 7. They've probably already started operations on a limited basis at the center. The intern program was not the Department of Defense's idea. It was actually pushed very hard by Senator Hagel, who said, "Okay, you're going to build a center and all the knowledge will stay in the center. How do we permeate private industry with people in the know?" Think about these interns. They might be looking at maritime transportation, but they're going to be rubbing shoulders with CEOs in global petroleum and global air, so these interns will now have a global perspective that extends beyond their particular sector. The private sector came to us and said, "You've got to have interns, because we want people to start permeating the private sector over ten years. If a problem hits, we won't be trying to find Williams or Jessica. We'll know whom to call and what to give them."

Oettinger: Before it slips my mind, let me interpolate another comment. You talk about interns, you talk about FFRDCs, you talk about trust, and you talk about how you and Jessica establish workable relationships with over a thousand people. That's an order or two of magnitude more efficient than what the ordinary operations directorate does with case officers who manage classical spies. The number of people whom any given case officer can effectively manage, build trust with, and hold onto over years and years is somewhere between ten and a hundred.

Williams: One spy doesn't broker the trust to the other spy.

Oettinger: Penetrating secrets is a couple of orders of magnitude less efficient than mining the open sources. This is an interesting concept, which I hadn't heard before.

Student: Can you imagine this center having access to the network in the private sector and a chief security officer calling you and saying "We're going out to Colombia or Indonesia. Can I speak to your point man there?" Can you imagine this center providing the same service to industry as it does to the U.S. government?

Williams: No, and the reason is that there are already mechanisms for that. The company would go to the Department of Commerce. If the company is going into, say, Colombia, there are mechanisms to get that information. Quite frankly, they are probably more efficient than ours, because they operate on a for-profit basis and they have the money to go out and hire the best person. If you want to get market access in Japan, you're not going to come to us and ask us how to do it. You will know that you have to get a Japanese distributor to get that access. So I can't see industries approaching us and asking us for that information.

They might want to ask about the present threat status of that country. That's already being done by the Department of State. They might ask, "Is this particular person whom we're dealing with dirty? Does he work for a terror organization?" It's already being done. So anything they can possibly ask us is already being done. What they gain from taking part in the PTDT, as I said earlier, is that they get a voice in the process. It might be minuscule, but they get a voice in exchange for about fifteen minutes of work maybe once every three or four years, so it's no problem to them.

Oettinger: You will get a chance to explore that from the other side: a private sector person who could comment on what they could get from the government versus other sources. That's Bob Liscouski. He was at one time in the State Department, dealing with embassy security and so on.[10] When he left the government, he became one of Coca Cola's major security people and then was the first assistant secretary of homeland security for infrastructure protection.

Williams: He's an interesting individual. When he first heard about this he wasn't a complete fan. After he heard more, he was actually the one who brokered the trusted relationship with Jim Caverly. That's how it works: one person brokering the next person, who brokers the next person.

I've talked about this already (**Figure 18**). The first two bullets are now either being done or are being attempted by other U.S. government organizations. I'm not saying it's because of the success of the PTDT, but other organizations are doing the first two and trying to set themselves up in areas of our expertise. Where we are still unique right now is in our access to the executives. If you want to get the information or broker the trust to the next person you really need the executive level.

You'll notice that the next three slides do not have the Strategic Command logo at the top left corner. That's because these are Williams's slides and I'm just throwing these ideas out to make you think about where we need to evolve.

We had Hurricane Katrina. Much of that has come to pass. What I want to show you is one of the courses of action that is actually out there, so now you have to use your critical thinking to find the problem with this mentality (**Figure 19**).

---

[10] See Robert P. Liscouski, "National Infrastructure Protection: Risk Management for a Nation in a Threat-Driven Environment," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2006* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, in press).

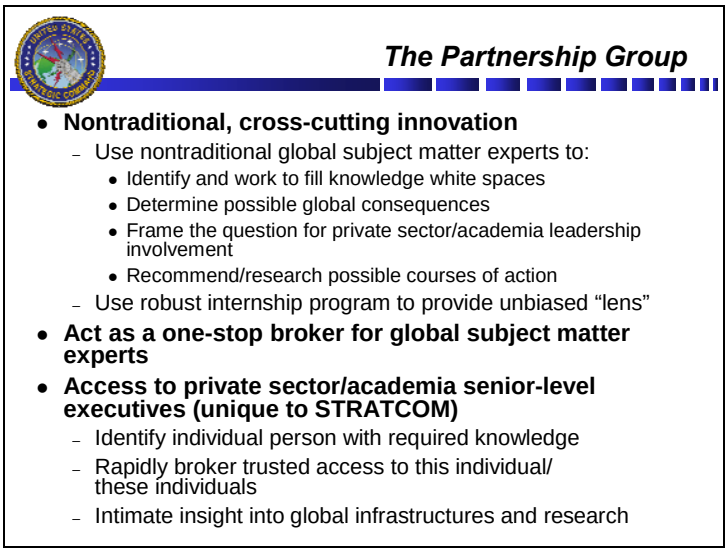

Figure 18

Figure 19

Business Executives for National Security [BENS] is a great, powerful organization for the private sector. They're working something called, I think, Super Metro Centers, Super Centers, or something like that, where they go into a metropolitan area and form a network of public-private partnering. They actually did it here in Boston for the Republican Convention, where they brought everyone together. They formed a network in New Jersey, San Francisco, and Los Angeles. Their idea in a post-Katrina world was "Why don't we build centers all around the United States, so that if another hurricane hits New Orleans we already have an integral public-private entity?"

I was working in the private sector a little bit after Katrina, asking what the problem is and what's going on, and discovered there were a lot of disconnects. If that network had already been set up, it would have been huge, but do you see any problems with this?

Student: You set up a network and it doesn't have anything to do.

Williams: It basically stays latent until it's required. It's like a war center. They would do exercises.

Oettinger: That's the beauty of what Darryl has described his center as doing. It's tapping people who in the ordinary course of their everyday activities have reason to do something and to do it right, because it's their livelihood, whereas here, as you pointed out, something lies dormant. It may or may not work. That's one of the reasons why an effective military corps has to exercise constantly, because otherwise it's kind of worthless.

Williams: These exercises are always going on. Every major metropolitan area is continuing to exercise its disaster response, but the private sector usually has very little play in that.

Oettinger: BENS has a Web site, which you ought to take a look at. It's www.bens.org .

Williams: I'll make this a little easier. We'll take out all but four of the centers (**Figure 20**). Do you see any problem yet?

Figure 20

Business Executives for National Security [BENS] is a great, powerful organization for the private sector. They're working something called, I think, Super Metro Centers, Super Centers, or something like that, where they go into a metropolitan area and form a network of public-private partnering. They actually did it here in Boston for the Republican Convention, where they brought everyone together. They formed a network in New Jersey, San Francisco, and Los Angeles. Their idea in a post-Katrina world was "Why don't we build centers all around the United States, so that if another hurricane hits New Orleans we already have an integral public-private entity?"

I was working in the private sector a little bit after Katrina, asking what the problem is and what's going on, and discovered there were a lot of disconnects. If that network had already been set up, it would have been huge, but do you see any problems with this?

This is the global precedent (**Figure 21**). This is the Department of Defense. You have Northern Command, Southern Command, Central Command, European Command, and Pacific Command. Each one has an area of expertise. What happens when you face a global threat? Who takes the lead?

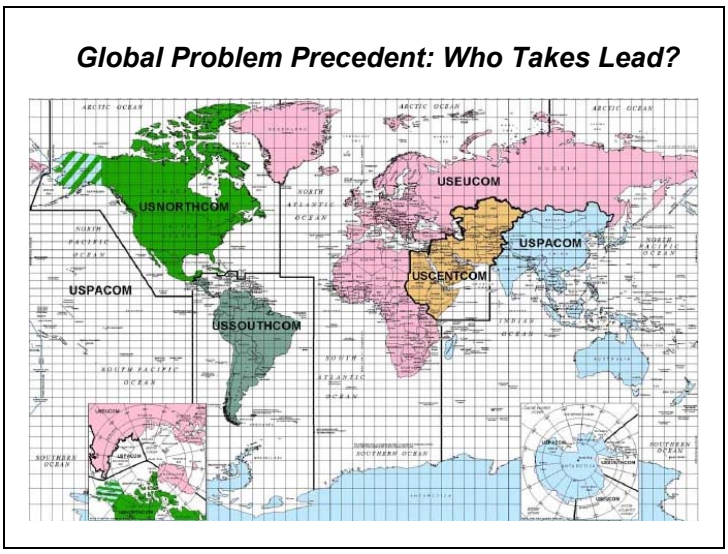

Figure 21

Let's say we have an insurgency or a problem at the Panama Canal. We know the money is coming from European Command, the container is right now in Pacific Command, and the command and control is actually coming out of Central Command. That's the problem we have. Southern Command would say, "Well, we take the lead." Central Command would say, "Well, no, we take the lead over here." This is why Special Operations Command and Strategic Command were given global missions: because of the need to integrate things across a global spectrum.

Now let's look at the previous slide (Figure 20). You set up a regional center to protect Miami in case of a hurricane. The hurricane hits. You've got your nodes set up and it works like a charm. You've got Wal-Mart sitting in the war room with Home Depot, and everything is moving great. But understand that you have a finite amount of resources, logistics, and everything else.

Now you have a terrorist who is opportunistic and blows off something in Long Beach. At the same time there might be an earthquake up in San Francisco. Now you have more than one calamity. Who takes the lead? You've got Wal-Mart mobilizing things down in Florida, you've got a problem in Long Beach, and you've got a problem in San Francisco. You have to have something at the national level.

Back in November 2003 we convened a round table in New York City to look at this particular problem (**Figure 22**). We had about eighteen people there. They were global leaders from all sectors, all elements of power, and we looked at simultaneous problems. How do you affect them? How do you marshal what you have to do? How do you get word to decision makers? Who gets priority?

That's when the Wall Street group actually said "What you outlined is nothing more than the problem that faced the Federal Reserve at the turn of the 1900s." We kind of scratched our heads and we sent a team of researchers to the Federal Reserve to read the communiqués from President Woodrow Wilson to J.P. Morgan and everyone else. We discovered that the same problem that we're running into, which we call a hurricane, they called money running. They had banks all over the country. If there was a run on one bank they couldn't get the money there fast enough, so they created the Federal Reserve.

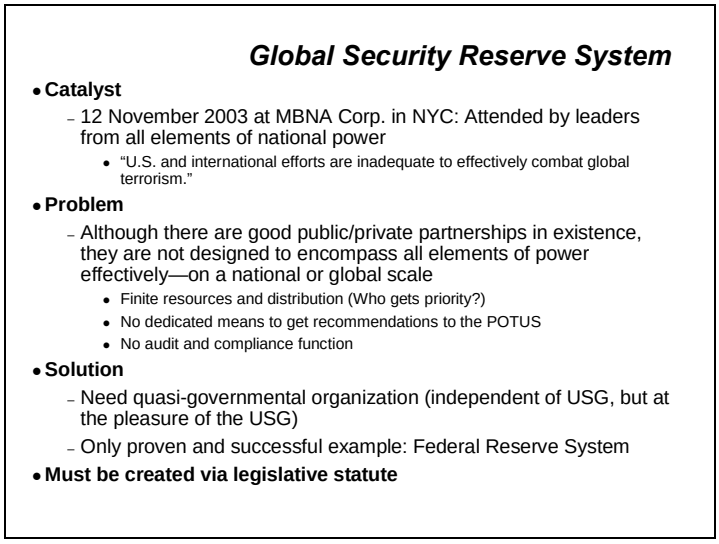

Figure 22

This is the plan: the Global Security Reserve System. If you read Steve Flynn's book, *America the Vulnerable*, he lists it as the Federal Security Reserve System. We would have regional boards set up under the FEMA [Federal Emergency Management Agency] separations (I think FEMA has ten sectors). Each board would be staffed with all elements of power specific to that sector. So, for example, in Sector 6, which is Texas and Louisiana, you have petroleum, shipping, and a few others. That regional entity would be looking at the vulnerabilities much as the Federal Reserve regional banks do. They would pass their concerns up to a national board composed of all regions, plus some U.S. government officials from the Department of Defense and so on, and some private sector entities. The national board would have a chairman selected by the president and confirmed by the Senate.

We presented this to Secretary Rumsfeld in the form of a white paper. Everyone seemed to like it, but it actually has to be accomplished through legislative statute. With the intelligence bill going through and a lot of the other stuff going on many of the CEOs who were trying to push this didn't get any traction. I want you to be aware that this is still out there as the private sector's recommended solution for handling simultaneous, physically separate disasters in the United States. It's just something for you to think about and chew over.

Oettinger: It's a fascinating suggestion. One difference that comes to mind is that the Federal Reserve problem is much easier in many respects, even though the structure looks the same. The resource that banks are dealing with is money, which is the most fungible of all commodities, and the metrics for success, the evaluation of need, everything, reduce to pure dollars. It's about as

pure a dollar problem as you can imagine, whereas you pointed out the regional differences and then the need at the national level to make judgments about the relative worth of different claims by the regions and the entities within them. There is no common denominator that's obvious in the way that the common denominator in the Federal Reserve system is the dollar.

Williams: You're absolutely correct, but it's remarkable how the politics that the Federal Reserve was dealing with mirror what we have today. The same question came up at the Federal Reserve level. Congress back then appointed a congressional advisory committee to look at a way ahead. I'm not too involved in this. I still listen to the private sector leaders. What they really would like to see is Congress appointing an advisory council just to examine the possibility.

I simply wanted you to be aware that right now all these solutions out there to correct Hurricane Katrina problems really fall apart in light of simultaneous attacks. I'm not an oracle, but so far this seems to be the only way that they continue to advocate. I think two of the CEOs actually went to Secretary Chertoff at DHS right after Katrina and talked to him about this. Once again it didn't get much leverage, because it is a long-term problem.

Oettinger: Most people think of the Federal Reserve system as being a government entity. They don't realize that it's one of those things that's somewhere between public and private. It's quasi-governmental.

Williams: Right. They do not want to be put under the U.S. government, but they want to be at the pleasure of the U.S. government. I think that's the way they describe it.

Student: I'm curious about your Global Innovation and Strategy Center. Is it run by an existing FFRDC or is it itself a new FFRDC?

Williams: No. It is run by Strategic Command at the pleasure of the combatant commander, General Cartwright. However, when you bring in insight from the private sector, you have to have a mechanism that will pass legal muster. That's why we have a combatant commander in charge, and under him we have a director—once again, a U.S. government entity. Under that, when you get to the subject matter experts, is where the FFRDC resides. It is just a conduit for the information coming in from the private sector.

Oettinger: Sort of an information laundry service.

Williams: It's a broker.

Student: What sort of budget and numbers of people are we talking about?

Williams: I won't go into the budget, because, quite frankly, I don't know, but I can go into the people. This is where we usually get the eyebrows raised. We have a very small group. If you read Thomas Friedman's book you discover that you don't need a lot of people in a Bangalore call center. You just need networks. Remember, this Global Innovation and Strategy Center is not only going to have a partnership group, it will also have a strategy group, an innovation group, and a few other groups that will take a task that someone wants us to do and make sure that task is accomplished. All we're doing is brokering. So our particular brokerage house at its maximum will have maybe twenty to thirty people, because all they need is to be able to broker. A stockbroker may handle 200 or 300 finance chains, but he is the single point of contact. We are going to have some redundancy in the brokerage, so finance will have two people and so on.

Student: What do you need to know, and how do you know it, about trusting one of the information assets?

Williams: That's a good question, because another thing that comes up is "What is the possibility that one of these trusted assets will impart information that will actually benefit them in the long run?" In the Federal Reserve, we know that bank XYZ is about to run out of money. That causes a run, and that gets into the system.

My background isn't in intelligence. (Actually I flew intelligence aircraft.) We have a rule that we do not accept one intercept as being gospel. If we get an indication that something is about to happen we do not consider that as gospel, because there could be a bias, or the person getting the information might put a bias into it. So we have to have corroboration from two independent sources.

So far what happens is that we'll get insight from an individual. We'll use two other individual sources to corroborate. If it's corroborated by three independent sources, we consider that information to be pretty reliable. We're never going to get 100 percent. We've talked to one intelligence agency that demanded 100 percent accuracy. I can't even tell you with 100 percent accuracy if I'm going to sleep on the right side or the left side of the bed tonight. You can't get 100 percent accuracy in intelligence until after something happens.

Student: That's what happens once that person is in the partnership. What I was asking was what you need to know about the people before you go to them, and how do you know it?

Williams: I guess the question is if we vet these people. To a point, no. It's usually just one trusted relationship with another. That's generally all we do, because we're only asking for process information.

Another question normally comes up: How do you keep the bad people from being part of this? You really have to describe what you mean by "the bad people." Many people in industry will be joint ventured and mergered and everything else with foreign companies, and through intelligence channels we will know that the other company does some nefarious things. Do we stop using that individual for insight?

Let me escalate it. Think about New York City and the its police commissioner, Ray Kelly. Ray Kelly has an individual embedded in Interpol. In Interpol you have Syrians, you have Libyans, you have the whole gamut. Do you stop using Interpol because it has contact with these people? Absolutely not!

We have to be aware of what people do, but since we're talking about global process information we haven't had a problem for the most part. Is it always a possibility? Yes; that's why we have intelligence oversight, OPSEC oversight, and legal oversight. But if one person will vouch for the other person, and then we can corroborate what that person gives us, we're usually okay. It's not foolproof and we still have to monitor everything we tell people.

Student: Historically, presumably, intelligence-gathering entities have always had some links with civil society. It may have been the master of an Oxford college giving MI5 a heads-up that an entity has done something. Is this just a recruiting arm of the federal government or of the intelligence gathering agencies?

Williams: That's good question, but recruiting means going to an entity and saying, "Will you help me, for my benefit only?" We're not recruiting anyone. These people, through word of mouth, actually come to us and say, "We have insight into a sector. If you can use it, fine. If you

can't, fine." We don't pay them anything. We don't offer them anything. For the most part they do it out of patriotism, and because they may actually be able to make a difference. They volunteer for us.

We've talked to the intelligence apparatus from Dr. Cambone on.[11] I don't like to look at the partnership as an intelligence entity. It is just a partnership for whatever the purpose may be. It might be intelligence. It might be insight. It might be facilitation. Avian flu is not intelligence; it's a hard core problem, and we're trying to form a consortium of private sector people to aid us in combating a possible pandemic. So I don't equate the two.

Student: You talked about concern over the fluidity of your contacts. Someone moves, through merger or acquisition, to a different company or a different area of the economy. Are you also concerned about fluidity within your organization? You're basing all these things on person-to-person contacts. What happens when people in your organization decide they want to get out?

Williams: The way we built the architecture is that there will always be a minimum six-month overlap before someone moves out. It's not like a university fellowship, where one person leaves and the next person comes in. Optimally (and "optimally" is always the keyword when you're talking about government ebbs and flows), it's built into the concept of operations that there will be a six-month overlap. During that overlap, at least in the directorate, we will go on field trips and we will broker the trusted relationships one to one. Since we have redundancy in every sector, it's incumbent on those two individuals to make sure each one is in the other's business and there is redundancy there. Is it foolproof? No, absolutely not. Is it the best we can do with the government budget? Absolutely, because we are really the slaves of budgetary dollars.

Student: Who gives you the tasks that you mentioned earlier?

Williams: The tasks could come from a myriad different places. Understand that the whole reason for our existence is to aid the commander of U.S. Strategic Command, but the potential resident in the partnerships far eclipses a Strategic Command or Defense Department focus. So the tasks usually come through the Department of Defense. The tasking for the avian flu came through the CDC. Most of them come in through a U.S. government entity, because we have to have a customer. We could sit around asking "What if?" and "What if" ourselves to death. We only have a few people.

One thing we do not allow, period, is harebrained contacts with these executives. We can't call Richard Parsons at Time-Warner and ask him "Have you ever thought about *this*?" He has just excused himself from a meeting and taken a phone call, and we ask him "Did you ever think about the price of rice in China?" After that, he is not going to accept our call the next time. It has to be a legitimate task from a customer.

We found that if we staff the center with subject matter experts they're a tremendous filter. They might say, "I can tell you what the price of rice is in China, because I've done that before." They also structure the questions. A lot of times we'll get an intelligence agency saying, "Hey, we want you to call Procter and Gamble and ask them *this*." "Well, what do you really want?" "We really want that information for this particular country." Okay, but for what product?" We'll interview the people who do the tasking so that when we go to Procter and Gamble we can say,

---

[11] Dr. Stephen A. Cambone is under secretary of defense for intelligence.

"We're really interested in how you sell laundry detergent to Country X." It's a very specific question. The person can answer it in fifteen minutes and it's done. So a lot of times what we do is actually enable the intelligence agencies to know how to structure a question.

Student: Do you have a group of people within your organization who think up tasks for you?

Williams: Right now, since we have so few people, we're so swamped that we really don't think about what might happen. If you just pick up a newspaper every day you can always find one or two things that will tell you what might happen. There is going to be an innovation group—actually, a futures group—and that is what they would do.

Student: You mentioned in your example taking tasks from the CDC or the Defense Department. Will you ever take a task from the private sector?

Williams: No, we will not. There are mechanisms for that out there, from the Information Sharing and Analysis Centers to Homeland Security to a lot of other things. When I really think about it, I couldn't imagine any task that they would give us. When it comes to marketing data and market access, they spend millions if not billions of dollars to get a competitive advantage. McDonald's will spend more than Burger King to make sure they get access. For them to come to us they would have to be aware that to be fair we're going to share what they asked us with everyone else. So I can't imagine anything they would ask, unless maybe they heard something, and then there are other mechanisms, through the FBI and so on.

Student: In relation to the futures department you were talking about, can you foresee in the next couple of years your projecting threats and then alerting the government, instead of responding to threats that they have identified?

Williams: Possibly. One interesting segue, and it's probably the last thing I'll say, is that this whole Partnership to Defeat Terrorism actually started as a byproduct of a master's-level research paper. I was asked in the year 2000 to stage a terror attack on the U.S. economy. My background is in accounting and international finance, so I thought, "Wouldn't it be cool to take down FedWire?" I was able to figure out how to do it successfully. At that point, the Federal Reserve would not talk to me until I sent them a notification. At the bottom of the Federal Reserve bank Web site there's a little Web master. I clicked on the Web master and said, "This is my name. This is my Social Security number. This is where I reside. [I was in Alabama.] I am about to publish a paper about how to take down FedWire for $1,500. Are you interested?" They messed up my wife a little bit, because a half hour later we got a call at home from the senior vice president of the New York Fed—and I never gave them my home number. He said, "You found our problem. You're going to be on a plane next week to fix it." Sure enough, I was on a plane and we did all the fixes about three months prior to 9/11. A lot of these vulnerabilities were already known.

Understand: if you go to the government with a paper, like that individual who mapped out the Internet, they will summarily classify your research, but you may get into things that are just astounding. What happened from that research paper is that we did a quid pro quo. I would introduce them to people in the government who would fix their problem if they introduced me to global financiers. Fast forward to 9/11, which took down the World Trade Center. They were looking for someone in the U.S. government who had contacts with global financiers and I just went from there.

You have a tremendous amount of power here at Harvard, because you've got time to do research and think about "What if?" Don't be afraid to ask people "What if?" and if anyone slams the phone down, as they did to me, take that as a challenge, because chances are that you found something they're trying to hide. But understand that they're going to classify your paper and it will never get published.

Student: From when you assume a task, is there a traditional life span or a time by which you hope to have it completed? Or is every task unique?

Williams: Every task is unique, but understand that we're just doing brokering for the most part. Most of our tasks go from initial tasking to completion in less than twenty-four hours. The reason is that we usually get the task at five o'clock at night and that's when everyone goes home, so we get hold of the people the next morning. The longest task we've ever had to do took us about a month and a half, and that was extremely complex. There were a lot of branches and everything else.

For most of the tasks that the government thinks are incredibly hard there is usually one person who says, "Oh, that's no problem. Here, do *this*," and hangs up the phone. We usually pull a Mr. Scott, as in *Star Trek*, and we won't give Captain Kirk the information right away. We'll wait an hour or two to make it look like we're doing a lot of work, but we have all the answers right away. It doesn't take long.

Oettinger: I trust that after hearing Darryl you have perhaps a different view of the enormous importance of the private sector as a source of information, whether it is through a mechanism like CNN or a mechanism like the one that Darryl has put together. Darryl, once again, thank you very much. I have a small token of our large appreciation.

Williams: Thank you very much.

Glossary

BENS	Business Executives for National Security
CDC	Centers for Disease Control
CEO	chief executive officer
CNN	Cable News Network
DHS	Department of Homeland Security
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
FOIA	Freedom of Information Act
HUMINT	human intelligence
OPSEC	operational security
PTDT	Partnership to Defeat Terrorism
UK	United Kingdom
Y2K	year 2000