

***INCIDENTAL PAPER***

## **Seminar on Intelligence, Command, and Control**

**National Security in the Twenty-First Century:  
An “All Elements” Approach  
Darryl R. Williams**

**Guest Presentations, Spring 2007**

William G. Boykin, Richard J. Danzig, James A. Baker,  
Warren G. Lavey, John D. Bansemer, Michael J. Sulick,  
Robert A. Fein, Darryl R. Williams, Rob Johnston

**December 2007**

# *Program on Information Resources Policy*



***Center for Information Policy Research***



***Harvard University***

The Program on Information Resources Policy is jointly sponsored by  
Harvard University and the Center for Information Policy Research.

*Chairman*  
Anthony G. Oettinger

*Managing Director*  
John C. B. LeGates

Copyright © 2007 by the President and Fellows of Harvard College. Not to be  
reproduced in any form without written consent from the Program on  
Information Resources Policy, Harvard University, Maxwell Dworkin 125,  
33 Oxford Street, Cambridge MA 02138. (617) 495-4114

E-mail: [pirp@deas.harvard.edu](mailto:pirp@deas.harvard.edu) URL: <http://www.pirp.harvard.edu>  
ISBN 1-879716-98-4 **I-07-1**

**National Security in the Twenty-First Century:  
An “All Elements” Approach**

**Darryl R. Williams**

**April 19, 2007**

---

Darryl R. Williams is the president and chief executive officer of Partnership Solutions International, a global problem-solving corporation. He is an internationally recognized expert in establishing architectures for information sharing between the global public and private sectors, countering terrorism’s exploitation of global infrastructures, creating global partnerships to solve difficult problems rapidly, and cross-pollinating existing or developing products into new or emerging markets. As an Air Force officer assigned to U.S. Strategic Command (STRATCOM), he was the architect of the Partnership to Defeat Terrorism (later called The Partnership Group), a network of global leaders from industry and academia dedicated to identifying and marginalizing terrorism’s attempts to exploit global infrastructures in order to further attack planning and logistics. Mr. Williams was also the co-creator of STRATCOM’s Global Innovation and Strategy Center, a world class collaboration facility that brings all elements of power together to solve the U.S. government’s hardest problems. Previously, he served as an electronic warfare officer specializing in offensive electronic attack, signals intelligence collection, and directed energy weapons. He has over 4400 hours of flight time, including combat and combat support, in both the B-52 and RC-135. He has traveled extensively in the United States, Europe, the Middle East, the Indian Ocean area, Singapore, and Japan. Mr. Williams retired from the Air Force as a lieutenant colonel in 2007. He has a bachelor of science degree in accounting, a master of business administration degree in international finance, and a master’s degree in military arts and strategy.

---

**Oettinger:** It is a great privilege to introduce to you our speaker for today, Darryl Williams. Sir, I turn it over to you. Welcome back!

**Williams:** Probably for the last time: I’m retiring. I don’t know if you were able to see the briefing I gave last year.<sup>1</sup> I figured that since it’s already on the Web the difficult thing for me to

---

<sup>1</sup> See Darryl R. Williams, “Combating Global Terrorism: Bringing All Elements of National Power to Bear,” in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2006* (Cambridge, Mass.: Harvard

do would be to come up with something unique. So I'm going to try a new briefing on you. If I look at the slides once or twice, it's because this is brand new: it's the inaugural one.

About two months ago I was asked to go out to IBM Research and give a presentation to all the research labs, on the subject of "What will business look like in 2010?" The reason they asked me to do that is because part of our job over the years of doing The Partnership Group is to interact with all of the CEOs [chief executive officers] of all the global infrastructures. As I was looking at the slides I put together for that presentation it struck me that in essence what I was outlining for business in 2010 is going to be the state or is already the state of terrorism. So in order to understand how to do national security now and in the future, we first of all have to understand how international business works. That seems to be the problem we've run into in government (not only in our government, but also in other governments): we try to attach a U.S. government or other government template to an activity that doesn't even fit that template. The right template is actually international commerce, international business, international movement of ideas and information. It has nothing to do with warfare against a nation-state.

So what I'm going to do today is overlay the presentation I gave to IBM with a national security focus. As we're going down this path, as we start talking about international business, commerce, and how to get ahead in the marketplace, I would like you to keep thinking about "Is this what the terrorists are using right now?" If you come to the same conclusion I did—that it is what they're using—then you can start changing your mindset as to what we as a country, and we as a world, have to do to start affecting this entity called terrorism or insurgency.

We have to start with paradigms. The previous paradigm, from the 1970s to the 1990s, is what I was taught when I was in school (my background is in accounting and international finance), and it is that everything dealt with scarcity (**Figure 1**). Scarcity of information, where there is only a finite amount of information, means that the cost to you as a company is how much money you are going to spend in order to get the information you need from that finite source.

Equate it to a child's game of "Go Fish." I don't know how many of you have played "Go Fish," but everyone has a deck of cards, and you try to guess what card that person has in his or her deck, and if you guess right you get to take that person's card and make a pair. That's what it is with scarcity: you basically have "Go Fish" with one to three decks of cards, and it's a matter of whether you can ask the right question to come up with the right solution. That is what Google and all your browsers are specifically built on: the paradigm of scarcity. If all of a sudden you aren't getting what you need, they put more processing power on it. So now they have bigger processors that can chug through the information faster.

Jeff Jonas<sup>2</sup> describes it as the equivalent of going to the Library of Congress and saying you need a book on Napoleon Bonaparte. You basically walk up and down every single stack and look at every single book until you finally find that book that says "Napoleon." That is what scarcity is all about, and that's what all these Web sites are based on.

---


University Program on Information Resources Policy, I-06-1, November 2006), [On-line]. URL: <http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=613>

<sup>2</sup> Jeff Jonas is IBM Distinguished Engineer and Chief Scientist, Entity Analytic Solutions, IBM Software Group.

**Previous Paradigm: Information Scarcity**

---

- 1970s–1990s
- Finite information flows
- Information cost: How much are you willing to spend to locate and secure most accurate information from a limited number of sources
  - Processing power, broadband/database access, and functionality are critical requirements
- Asking the best question is key to success
  - “Go Fish” with 1–3 card decks




**Figure 1**

The paradigm of warfare is the same (**Figure 2**). You have the nation-state, and nation-states have very specific processes. They have a process called “rail.” Nazi Germany, for instance, had a process called “ball-bearing plants.” You can attack those processes, and there’s very little collateral damage, in the sense of damage that goes outside the country’s border. That is the paradigm that we used to engage with national security.

**Previous Paradigm: Warfare**

---

- **Warfare Was Conducted Against Established Nation-States**
  - Adversary Used Indigenous or Captured Logistic Processes to Continue War
  - Collateral Damage Limited Due to Inherent Isolation




**Figure 2**

Now we get to the new paradigm. A lot happened in 2001. In 2001 three individuals won the Nobel Prize in economics for “Analyses of Markets with Asymmetric Information” (**Figure 3**). It really set the whole world on its ears, and business is still trying to catch up.


**Asymmetric Information:  
The 21<sup>st</sup> Century Paradigm**

---


2001 Nobel Prize in Economics:  
*“Analyses of Markets with Asymmetric Information”*



Dr. George A. Akerlof  
UC Berkeley



Dr. A. Michael Spence  
Stanford



Dr. Joseph E. Stiglitz  
Columbia

**Why is this important?**

**Figure 3**

The reason why is that you no longer have information scarcity, you have information saturation (**Figure 4**). Now you have global pipes of information—a tremendous amount of data. The information cost is how much time you are willing to spend to separate the wheat from the chaff; it’s no longer how you can find what you want out of very finite data pipes. You have incrementally escalating numbers of data pipes, and more being added every single minute. Now you have the same “Go Fish” scenario, but instead of three decks of cards you have thousands of decks in different languages, with different pictures, and as you’re about to ask the question three or four new decks of cards get thrown at you, all of them different. You don’t even know what question to ask, let alone where you’re going to go.

**21<sup>st</sup> Century Paradigm: Information Saturation**

---

- **Exponentially increasing information sources and flows**
- **Information costs: How much are you willing to spend to locate and secure most accurate information from an ever-growing, global pipeline of information? “Wheat from the chaff”**
- **Have no idea what question to ask**
  - “Go Fish” with 1000s of card decks with different languages, pictures, and rules
  - Increasing processing power and search criteria will eventually give you the correct answer, but at what cost of time and how long will it take?
- **Asking the right question and non-obvious relationships are the keys to information search success.**

**Figure 4**

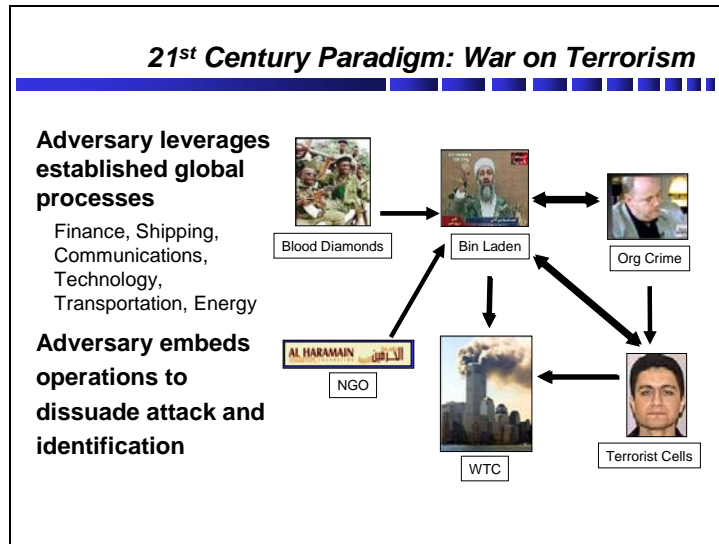
With Google and these others, when you type in a question it gives you a question back: “Did you really mean *this*?” That is Google and all these other browsers trying to make an information scarcity model equate to the information saturation model.

What you’re really looking for are nonobvious relationships. For example, in a lot of the research I do I’ll type in a place. Let’s say I need to know about Prague. The search engine will come back and give me everything about Prague, Czechoslovakia, but let’s say I’m really talking about Prague, Nebraska. Did I really mean “Prague”? Did I spell it right? It’s really crazy when you have to ask the browser the exact question in order to get that exact answer. Many times, if you’re like me, you’ll spend hours asking the browser the same question. “Let me put in this word instead of that word. Let me put another verb in here.” Then when you finally find it, and your computer crashes, you have a very difficult time getting back to that same Web site, because you have to go through all the questions again.

Increasing the processing power and the search criteria will work in the interim, but it will eventually reach a point where it’s ridiculous. IBM has just created the Blue Gene computer, which is the most powerful computer on the earth now. But even the Blue Gene computer will rapidly get swamped if you open it up to global reams of data. Let’s say they just bring in finance data, which is \$6 trillion per day of information. Then let’s say you add in all of the data from AIG Insurance. Then you bring in all the bills of lading of every containerized shipper in the world. There are 60 million containers in existence at any given time. You see where I’m coming from? I was at the AT&T Global Network Operations facility, and they’ve got a three-story facility just to try to get their arms around all the data going through their pipes. Add that to your data store. How much processing power can you possibly create to give you the answer you need?

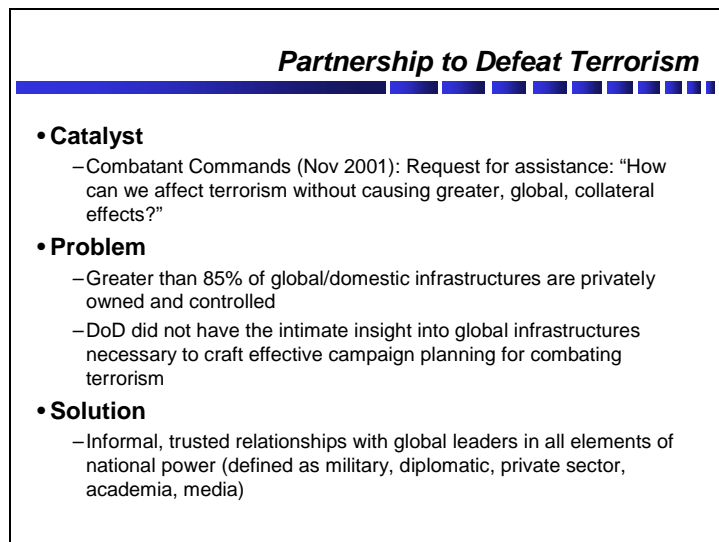
Now let’s go to September 11, 2001. Understanding that you have these global reams of data, you have a situation where most of our world is operating on information scarcity. Even the intelligence community is operating on an information scarcity model. Part of this model is \$6 trillion a day in transactions. Now you have a terrorist who is only spending \$9,999 to keep under the ceiling for suspicious activity reports. How are you going to find that \$9,999 in a stream of \$6 trillion? You can’t. So basically what the adversaries are doing is embedding their processes—movement of people, money, materials, ideas, and ideology—and burying them in that huge pipe that is continuing to increase exponentially (**Figure 5**).

Even if we were to find it, how would we do anything about it? Do we just go into the monetary pipeline and say “Everyone stop, because we need to take care of this \$9,999 transaction”? Meanwhile we’re bringing global commerce to a standstill. Now we’ve caused a greater global collateral effect just to affect this terrorist operation. I don’t know if you see where I’m going with this. The idea is to find the incursion and stop it, while allowing the rest of the business to continue.



**Figure 5**

That's why we created the Partnership to Defeat Terrorism [PTDT] in 2001 (**Figure 6**). It actually began as a project to help the Federal Reserve protect its monetary transfer system, but it really started in full force right after 9/11. At that point it was like the whole world woke up at the same time. The combatant commanders, the four-stars, who control vast regions, woke up and said "I have an adversary whom I have to stop." In the case of European Command, the combatant commander said "I have an adversary who recruited the 9/11 terrorists out of Germany. How can I detect them, how can I stop them, and how can I close down the whole system without causing a greater global collateral effect?"



**Figure 6**

The answer is that they can't. Many times we in the government feel that anything that can possibly be done we can do inside the Beltway in Washington, D.C. It doesn't work that way. I

would say we're ahead of most governments that are trying to do the same thing. The reason why it can't be done is that 85 percent, if not more, of all global infrastructures are owned by the private sector. You cannot go in and exercise eminent domain over a global infrastructure. It just doesn't work. We as the DoD [Department of Defense] did not have the insight we needed to understand, first of all, how their process works, let alone ask the right questions to detect some incursion into that process.

The solution we came up with is trusted, informal relationships. We found that there was a very large group of basically frustrated (I don't want to call them disenfranchised) chairmen and CEOs who had lost friends and family in 9/11. They wanted to help the government. Let's just pick a person, such as the head of Citigroup. If you look on Citigroup's Web site, they're not only a huge power when it comes to finance, but they're also a huge power when it comes to sharia-type business, or Islamic business. They have a tremendous role to play when it comes to understanding the mindset and how you move money in a sharia matrix where it's not based on profit and loss, but on profit sharing.

We built these trusted relationships, and we started going out to one or two CEOs and asking "Can you help us? We don't want your privacy information. If you're FedEx, we don't care how you do things faster than your competition. We just want to know how you do business from Point A to Point B." What we found is that we had tapped an untapped niche. You'll see how the process works in a couple of minutes.

They give us insight. We give them a question that to us in the government is extremely hard, but to them it's what they do on a daily basis. For example, I work with PCs, but if I were to go to someone with an Apple laptop and ask "How do I boot up an Apple?" to that person it's mundane information. So for these people who work in finance, or containerized shipping, or any one of these other global infrastructures, it's their daily business. To them the information they're giving us is very mundane, but to us it's like the light from a light bulb.

We'll get into how we do that, but we get global leaders in all elements of national power. If you read any of the literature put out by the U.S. government, we define "elements of national power" as diplomatic, information, military, and economic [DIME]. We started going out to the private sector with that definition and we were basically laughed out of the boardroom, because it really is irrelevant. Whether you are doing a finance transaction, making your airline reservations, or talking on the telephone, information is not an element of power, it's a commodity. It's what makes the world move.

The private sector defined it in the following way, and this is the definition we use: "elements that use information, and can use information, to influence the nation-state or the globe: that is, military, diplomatic, private sector, academia, and media." We have media in there, which is sometimes a bad word, but we found that media is a critical piece.

You always have to have a mission (**Figure 7**). The bottom line is that we partner to provide options. Those options are for the president, the secretary of defense, the combatant commanders, or even the sub-commanders. Our mission for the most part is to support the Department of Defense, and specifically U.S. Strategic Command.



**Partnership to Defeat Terrorism**

---

- **Mission Statement**
  - Partner with academia, international global process leaders, and media experts to provide the POTUS, SECDEF, and Combatant Commanders with options for combating terrorism that cover all elements of national/international power
- **Fills critical need:**
  - Brings fidelity to intelligence chatter
  - Supports the development of counterterrorism actions
    - Feasible and effective
    - Consequence management
- **Global view versus domestic view**
- **Keys to success: Trust + UNCLASSIFIED + Virtual = Rapid Results**

**Figure 7**

So the first three years were kind of bloody, but now we've basically mapped out the minefield and we know where we have value. The value is that we bring fidelity to intelligence chatter. The chatter you hear in the news every once in a while is just that: it's random messages or intercepts that are just a jumble when you put them all together. When you bring them to the private sector it brings fidelity.

We support the development of counterterrorism actions, and also determine if those actions are feasible and effective. For example, you might say "I want to stop a financial transaction by blowing up a bank." Since you don't know anything about financial transactions, blowing up the bank does nothing, because you're talking about bits and bytes of data moving, not actual money. There's also consequence management. If you do something, will it cause it cause a greater global collateral effect?

We focus on the global view versus the domestic view. We get a lot of questions about "Isn't the Department of Homeland Security [DHS] doing this?" Yes, but we look at things globally, while DHS looks at it from the borders in. Petroleum companies are very concerned about the refineries and pipelines here, but they're as concerned, if not more concerned, with their whole system. It could be their oilfields in the Caspian Sea or in the Indonesian area; it could be their tankers; it could be pipelines; it could be a whole lot of things.

There are several keys to success. You're never going to get away from trust. You can try to institutionalize some pieces and put a new name on something, but really, when it comes down to it, it's trust. If you are going to move on to a job or a position, it is imperative that you have overlap with the individuals taking over your place. It's not a matter of calling up Bill Gates at Microsoft and saying "Hey, Bill, I'm going to put someone on the phone. Talk with him." He's going to hang up on you. Instead, you go out there and sit down with him and say "You've worked with me for quite a while. I'd like to introduce you to my replacement." Then they talk, and they build up trust.

It has to be unclassified. Many times we love to classify things. If a terrorist burps, we will put “Top Secret” on it, because maybe it’s in a different language and we can get something out of it. These individuals don’t have time to get clearances. They might be in Milan and they have fifteen minutes to talk to you on a cell phone. They don’t have time to do it over a classified medium.

Also, it’s virtual. Governments tend to like to get everyone together face-to-face. That way we can do the secret thing: if we tell one person a secret and pass it around the room we get to see everyone and talk to everyone. That’s not the way the world works. The way the world works is all virtual. I think that Thomas Friedman said “The world is flat.”<sup>3</sup> I beg to differ: I think it’s a dot. “Flat” indicates that there are length and breadth.

We were tasked to come up with a concept of operations and we were given over the New Year’s holiday to do it. We couldn’t physically convene a group of CEOs to do it, so we actually convened virtually. We had the former commandant of the Marine Corps in Delaware with a laptop. We had the former dean of the Kennedy School here with a laptop. We had a company chairman who blew out his knee on the slopes in Vail who communicated with us over a Blackberry, and so on and so forth. We got together virtually, passed files back and forth, and within forty-eight hours we had an airtight document. That’s the way life works today. It’s virtual.

This is how we in essence work (**Figure 8**). If you use a hierarchical structure, where the president gives a task to the four-star, the four-star gives a task to my superior, my superior gives the task to me, and then I give the task to someone else, it will take forever until you get to the individual who actually knows what you’re talking about.

For any problem, there’s one person out there in the world who is the expert on it. We were talking in D.C. about two days ago about a mudwort (I guess it’s a plant).<sup>4</sup> There’s actually an expert out there on mudworts, but to find that person would take days. What we do is energize nodes. We go to academia and say “We need to know who’s an expert on mudworts.” They, in turn, will energize all of their nodes, and so on, and it feeds back on itself, so within hours, if not minutes, they will say “You need to talk to this individual at this university. He is *the* expert on mudworts.” You call the individual up and get the information, and it’s very, very fast.

---

<sup>3</sup> Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-First Century* (New York: Farrar, Straus and Giroux, 2005).

<sup>4</sup> A mudwort (*Limosella aquatica*) is a small herbaceous plant that grows on muddy shores.

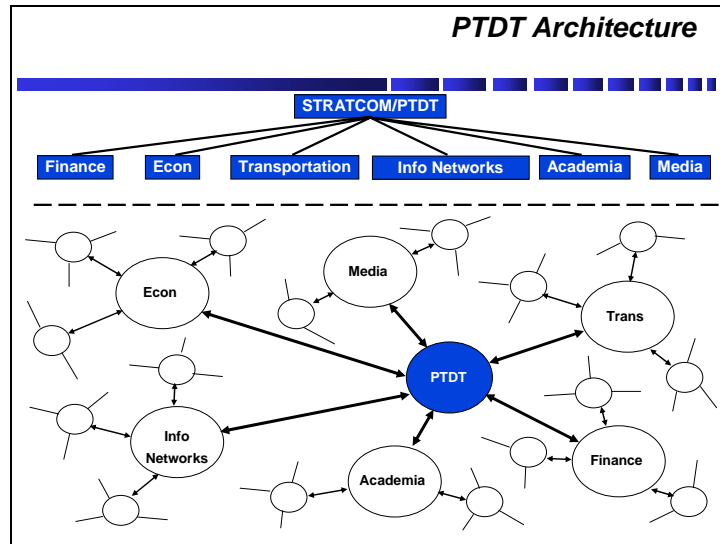


Figure 8

But there are also huge legality problems (Figure 9). If you ever want to have an interesting discussion, type in "Total Information Awareness," or "TIA." It was a government effort to do all-encompassing information Web crawling with the private sector. There are huge problems. If the public sector maintains the database, then you have problems with the Freedom of Information Act [FOIA]. Let's say that Citigroup sends us inside information on their company. They're giving it to the U.S. government. We could probably beat the FOIA request, but it still is open to FOIA.

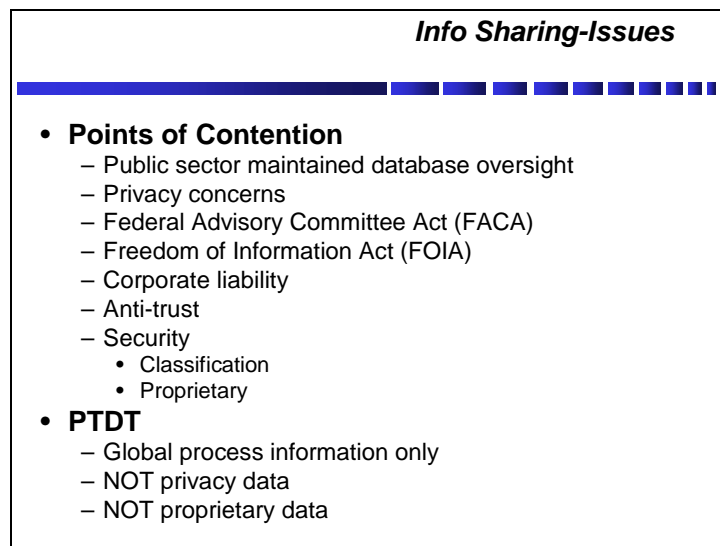


Figure 9

What if we allow the private sector to maintain all the information and we give them classified information? They get together and form a consensus, and say "We as a group will tell the U.S. government 'You should do *this*.'" Now you're up against the Federal Advisory

Committee Act [FACA], which was intended to stop power brokers back in the 1930s, such as J.P. Morgan, from getting together and telling the government how to operate.

You have privacy concerns. Do you really want your information held in the reliable hands of a government? No. You have corporate liability. You have antitrust. You have security. There are ways to rectify this. The Markle Foundation did wonderful work on how to rectify this without compromising anything, but we don't get into any of this. At The Partnership Group we deal with process information only: how do you do business from Point A to Point B? We don't deal with privacy data or proprietary data. That doesn't mean people haven't offered it to us, but we don't deal with it. We give it to the proper sources that can handle it.

This is one of few unclassified examples that I can give (Figure 10). Most questions about terrorism that come to us start as classified. When we go into the private sector they're unclassified, but when it all comes together and we have results it goes back to being classified.

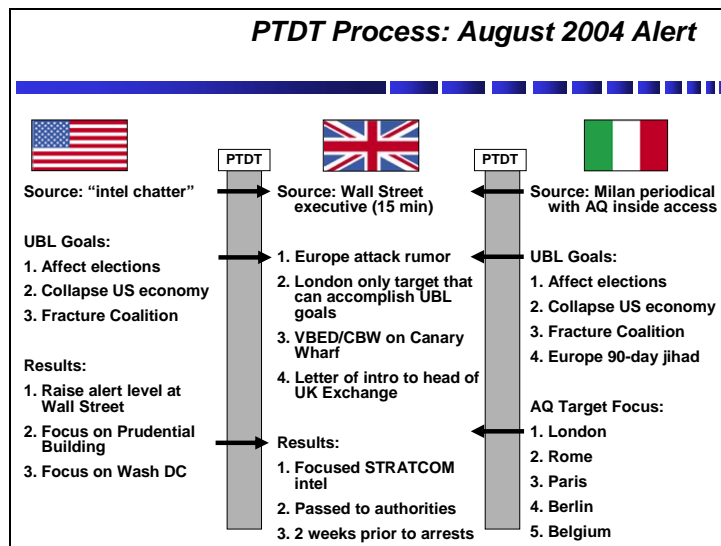


Figure 10

Here we had a situation where we had a conflict. This happened back in August 2004. I don't know how many of you remember this, but a laptop was intercepted (I don't know how), and on the laptop there were a lot of pictures of Wall Street, the Prudential Building, and Washington, D.C. On that basis, we increased the terror alert, we increased the security around the Prudential Building, and it was news everywhere.

At the same time, there was a journalist in Milan who was about to publish an article saying that the attack was not going to be on Wall Street; it was going to be in Europe. We don't know the reason why he knew (maybe he had inside sources) but he said his sources were saying that the target would be London, Rome, Paris, Berlin, or Belgium.

So we had a conflict. What should we do? At that point we got the call: "Can you give us fidelity on what's going on here?" It was much like *Mission Impossible*. We went through our Rolodex. We needed a financier who's a world-renowned expert on investment banking,

exchanges, and whatever else. We found one: a Wall Street executive. We actually met with him last night. He's an interesting individual.

Each one of these leaders gives the Partnership an access number. That access number gets us past all of that bureaucracy directly to his Blackberry or his pager. So we operate on about a sixty-minute benchmark from the time we are tasked to the time we get that chairman or CEO or academic leader on the phone. In this case it took fifteen minutes. He got on the phone and I read him both unclassified transcripts and asked him, "What do you think?" He said, "It's funny that you should mention that, because we also monitor chat sites." You find a lot of intelligence through the private sector. He said "We're actually gearing up for a European attack versus a U.S. attack." Then he went through all of these regions, and he said "If they're going to hit any one of these, they're either going to attack Belgium or London. The other ones really wouldn't do anything to the economy." We always have to remember the terrorists' goals, and the goal here was the collapse of the U.S. economy. He said, "If I were to do it, I would use a vehicle-borne explosive on Canary Wharf, because you have to kill leaders versus destroying buildings." From there he brokered an introduction to the head of the UK [United Kingdom] stock exchange. That's all the information we needed.

Remember information scarcity and the "Go Fish" analogy? The intelligence apparatus is very good for forensics. Once 9/11 happened, it was very easy for us to go back and determine where we missed everything, because the model is based on information scarcity. Now we go back to intelligence with a question: "Is there an Al Qaeda cell operating in London?" Well, once you ask a question like that, immediately a flag comes up and they say "Oh, yes, there is." We were then able to send the information to the authorities. This happened about two weeks before the arrests. It did not lead to the arrests. We had actually been over in England and briefed all the way through their government. They were well aware of this, but we were able to show them that when you bring all the elements of power to bear you can rapidly uncover things that for the most part are very hidden.

Remember that institutional piece? There is a problem if you don't institutionalize the architecture, and that is that you have single points of failure. If that individual who has a node meets an untimely demise from the front end of a bus or something, that whole node goes away. Now you've got a problem. So the private sector contacted the four-star general who commands U.S. Strategic Command, General James Cartwright. He did not ask them to do this, but they sent a letter to him saying that they wanted to institutionalize the Partnership, and if he would institutionalize it they would throw their weight and credibility behind it.

He called their bluff. He picked a date ten days away—one of the coldest days of the year in January—for them to get to Omaha, and they showed up, along with the two senators from Nebraska, representatives from DHS and Northern Command, and even a Harvard dean. We went through the scenario, and we came up with this building (**Figure 11**). It was called the Global Innovation and Strategy Center [GISC].



**Figure 11**

What it does is institutionalize one of three necessary pillars. The first pillar is the day-to-day task of bringing fidelity to intelligence chatter, and being able to help senior leaders phrase a question. A senior leader might come to us and say “We need to stop financial transactions between terrorists.” You can’t go to the chairman of Bear Stearns and say “Tell me everything one has to do to stop financial transactions among terrorists.” There isn’t enough time in the day, and he’d probably hang up the phone. What we have are subject matter experts, people painstakingly hired as experts in their field, who can look into the question and frame the problem in a more focused question with which we can then go out to a CEO. It makes things a lot different from the old “Go Fish.” Now we have a proper question.

It also institutionalizes connections between the mid-level workers of a corporation. In the case of containerized shipping, where Maersk does 60 percent of all containerized shipping, our maritime subject matter expert has a very tight relationship with his counterpart in Maersk. So if we have a transportation problem, he can immediately call that individual.

That’s been institutionalized. However, the other two legs you can’t institutionalize, or, if you can, it can’t be done very rapidly. One is almost like what a couple of nights ago I described as the Minutemen and the militia. Here we are in Massachusetts, and in 1775 the Minutemen were all civilians one minute and the next minute they were out on the bridge with muskets and were now the military.

In the Partnership, the Minutemen are the chairmen and CEOs, who for the most part conduct their daily business for days, months, or years. Then one day you will get a hard problem, a crisis problem—say, Hurricane Katrina, or an impending terror attack, or even a response to a terror attack. You immediately need to get access to these chairmen and CEOs, get their insight, and maybe get their cooperation for a couple of hours or a couple of days. Those are the ones where it’s based on trusted relationships. They’re not going to pick up the phone just because you’re from the GISC, but they will pick up the phone if they know you and you’re kind of a friend of theirs.

It's much like if I came to you and said "I'd like to have the name and number of your mother," then went to her, and said I'd like the name and number of her aunt, and then called the aunt directly. First of all, she's not going to pick up; she'll probably think I'm a telemarketer. That's the way it is in industry. These chairmen and CEOs are controlling multibillion-dollar corporations, and if they don't know who you are they're not going to talk to you. So that's your Minuteman pillar.

The last one is to get groups together that actually think forward. You get a group that includes the head of Goldman Sachs, the head of Union Pacific Railroad, and the head of American Airlines—about twelve people altogether—and sit down and talk about where they see their industry moving and where they see the threats emerging. That particular thing is being done very well by a group called the Highlands Forum.<sup>5</sup> That's long-range thinking; it's a one-time event where you pick a problem, bring these people together, and they come up with a strategic plan.

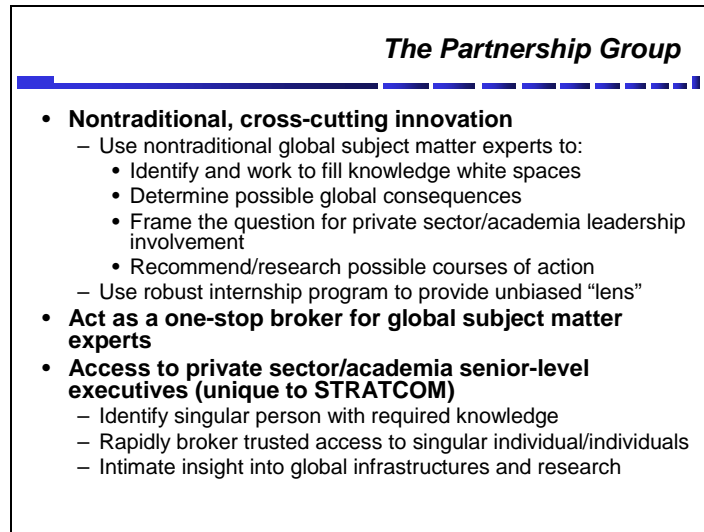
The GISC does the first pillar. It does it very well. Because of our trusted relationships with the chairmen and CEOs we can also do the second one. I personally believe that second pillar should eventually migrate upward to a higher level strategically: maybe under the Executive Office of the President or somewhere else, because you have to be able to cultivate these relationships. That's just my personal opinion.

I already talked about The Partnership Group (**Figure 12**). It's basically a brokerage house: come to us with your tired, your heavy laden, your weary, and we will give them rest. If you come to us with your problem, we will use our network to find the one person who has the answer, broker the two of you together, step away, and let you come up with the solutions.

One thing that's interesting, though, is that we started an internship program. I wish we could claim that internship program was our great idea, but it wasn't. It was pushed very strongly by Senator Chuck Hagel from Nebraska and even more so by chairmen and CEOs of Fortune 100 companies. As they looked off into the future at the threat they recognized that it would behoove them to have a new hire at the mid level who is not only aware of their particular niche, like investment banking, but is also aware of what's going on in petroleum, in transportation, and basically has a bird's-eye view of all global infrastructures. They're the ones who really pushed this, and we have our first internship class, who are about to give us their results. They're looking at communications processes in Pan-Sahel Africa. How do you move information? They looked at everything from tribal drums to cell phones. It's amazing work, because they have time actually to research it. So this is an area that is starting to pick up a lot of steam.

---

<sup>5</sup> For background on the Highlands Forum, see Richard P. O'Neill, "The Highlands Forum Process," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, December 2001), [On-line]. URL: <http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=563>



**Figure 12**

Now we get to the world of 2010. The first thing we’re going to do is look at business in 2010. Where does business have to go? As you look at these slides, think “Is this what terrorists already know, and we’re trying to play catch-up?”

If you’re going to succeed in business in 2010, you have to have cross-sector, global alliances (**Figure 13**). You have extremely finite logistics. If you think about a terrorist organization, it’s very broad, but it’s very shallow. You might have one financier; you might have one logistics individual. The only way that terrorist organizations can actually conduct an attack—think of 9/11—is to have cross-sector alliances. They have an individual who is very good at documentation and another individual in another part of the world who is very good at making travel arrangements.



**Figure 13**

I’m about to retire, and I’m building my own company. I went to a Web master, which was an eye-opening experience. Understand that I’ve been with the Partnership for seven years now. I



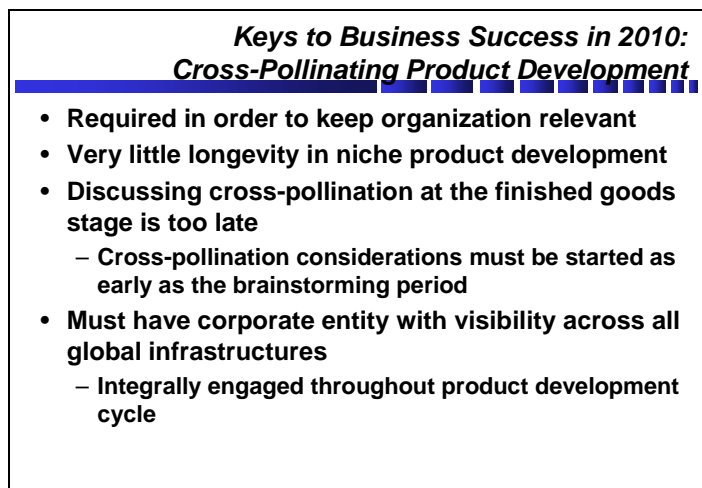
thought that Web master would sit down with me and get all of his group together in a semicircle, I would tell them exactly what I want, and they'd break up and build a Web site for me. We went out to lunch, and he asked "What do you want to say?" We went through that, and he said "Okay, got it." He then called up a content manager in Europe. They were talking back and forth to each other on the Internet about building this Web site. Now we needed a new logo, so they talked to someone in New Zealand, who is their foremost graphic artist. He got tired of the corporate world and is building Quonset huts, I think for the Peace Corps, in New Zealand, but his night-time job is to do graphic art for Web sites. Another of their graphic artists is in India. So I went to an individual in Omaha, but the package I'm getting back is a cross-sector global alliance to give me my Web site. They were able to do it very fast: faster than I could ever have managed. By the time I left that lunch and got home I already had a skeleton of a Web site up. It's amazingly fast. As I told IBM, if you're going to be able to compete you have to have cross-sector alliances.

What do I mean? For example, trucking firms were starting to see a lot of their competitive advantage go away. The reason why it was going away is that if you want to compete globally you have to rely on certain things. First of all, their trucks cannot operate in the ocean, so they have to rely on shipping. To get things there faster they made an alliance with a shipping company. Now they can track their package from when it's picked up on a doorstep in China to when it's dropped off on a doorstep in the United States. That gave them an advantage.

Containerized shipping is so precise when it comes to times that rail and truck and everything else rely on the time when that ship comes into port. So if bad weather delays the ship, there has to be a way of stopping trains, redirecting trucks, and everything else. They're all tied together in one network now.

So if the terrorists are going to compete and be successful, they have to have global alliances across sectors. Think of Al Qaeda. Al Qaeda is like a box of Kleenexes; not a box of chocolates. (It doesn't matter if you have Kleenex or Puffs or Brand X tissues; everyone calls them Kleenexes.) Al Qaeda is the same way. Everyone says that everything is Al Qaeda. There's Al Qaeda with some operations in Iraq; Al Qaeda with operations in the Philippines is called Abu Sayyef; Al Qaeda in Indonesia is the JI [Jemaah Islamiyah], and so on. Each one has a specialty. One might be in building bombs, or documents, or whatever else. They've learned it; we have to learn it.

For business success you have to cross-pollinate your product (**Figure 14**). This is the biggest problem right now in global business. Because of all the mergers and acquisitions, most of your corporations, say in telecommunications, have for the most part saturated their niche, yet the chairman and CEO want them to continue to fight for growth. The only way you can do that is to take a product that is designed for telecommunications and pollinate it over into, say, transportation or something else. Some companies that I talked to are trying to do it after they've already built the product. We see it a lot with gaming systems, where they build it to the specifications of, say, Japan, but when they bring it over here it just doesn't work and everyone gets mad. I'm still waiting for Halo 3. I think it's going to take forever. I guess the Beta version will come out on May 11. So when they try to migrate that to a different country things don't work.



**Figure 14**

You have to look at cross-pollinating your product during the product development phase, the brainstorming phase specifically. Think about the roadside bombs over in Iraq now. It doesn't matter what we do; they're already thinking about the next step of where they're going to go. So we might build a new kind of jammer, but they're using something different, because they're moving faster than we adapt.

I was in a brainstorming session two days ago, and the CEO of a biotech company brought up something that I told him I was going to use when the time was right. I guess the time is right. He made up something called I<sup>4</sup>: ideas, innovation, implementation, and imitation. It is the product cycle. It's how long you are going to have a competitive advantage. Up until a couple of years ago, that cycle, I<sup>4</sup>, was thirty years. If you had a new technology, you had a competitive advantage for thirty years before an imitator came along. In his last survey he said that cycle has gone from thirty years to thirty weeks. Compare that with a government acquisition cycle, which deals in years. We were all amazed when the F-117 and the B-2 came out. In essence, when the F-117 came out in the 1980s it was actually 1970s technology, so it took ten years to bring it to bear. Now you have the adversary in business working in a thirty-week cycle. By the time you get to imitation they're going on to the next idea. Think about that! We have to get inside the thirty-week cycle. We argued in the brainstorming session that it's probably less than thirty weeks now; it's probably down to maybe twenty weeks. We have to get there.

Academia must be empowered (**Figure 15**). What we have found is that your best ideas are in academia. If you talk about a thirty-week cycle, business doesn't have a lot of time to spend on thinking, but academia spends a lot of time on that. So we actually have to take on a venture capital mentality, where we go through academia and find the best ideas. Many of these ideas only need about \$5,000 or \$10,000 to push them to the prototype stage. Funding for academia keeps getting cut all the time, but for \$10,000, \$20,000, or even \$50,000—which is chump change when you think about the budgets of many of these Fortune 500 companies—they can give you a prototype of exactly what you need. Academia is the solution.

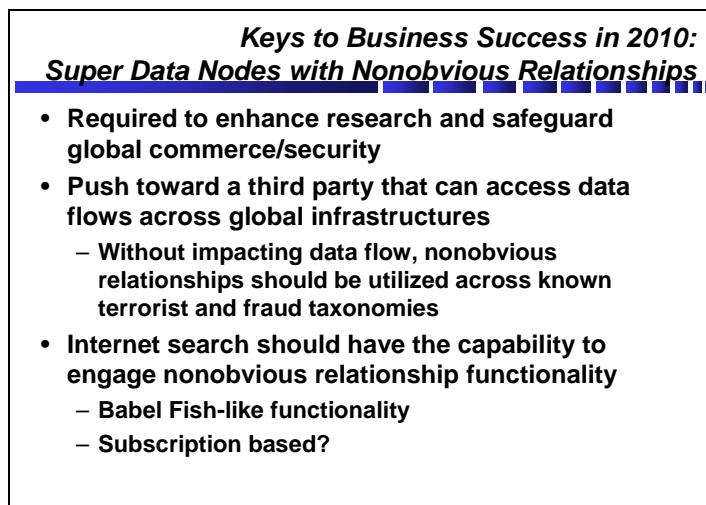


**Figure 15**

We were tasked by the CDC [Centers for Disease Control and Prevention] to come up with a brand new surveillance model to detect avian flu. They only gave us 120 days to do it. If we had used a typical governmental structure and gone out for bids, the bids alone would probably have taken 120 days. We went to academia. They brought in a high school senior, a college freshman, and a college sophomore. Within two weeks, during their final exam periods, those three individuals created a surveillance model that the CDC adopted. We can't do it that fast, but they can. They have the time and the knowledge. So academia must be empowered.

If you think about terrorism, where are they getting their recruits? Academia. Madrassas. A lot of the other areas.

The next one is nonobvious relationships (**Figure 16**). This is how you detect terrorism. The terrorists aren't really using this, but we need it to detect them. When you have something buried in a stream of global data, the only way you're going to detect it is through nonobvious relationships. What I mean by that is that you have an individual who has the same address as another individual who works at the same company as another person, and that company has the same phone number, and so on and so forth, so you finally get the six degrees of separation of Kevin Bacon. You have an individual who conducts an action, and once it goes through all the relationships that action is actually designed to conduct a terror attack. That's the only way you're going to find it. If you're going to do Internet searches in a world of information saturation it has to be with nonobvious relationships.



**Figure 16**

I foresee the Babel Fish-type functionality. You type in a question: “Tell me everything there is to know about mudworts” and it will do nonobvious relationships. “Mudworts are part of this genus; they grow in this country; this country has a football team; this football team has a coach, the coach’s nickname is ‘Mudwort.’” Basically it does all of those nonobvious relationships and the only thing we might know in intelligence is “mudwort” and “conduct operation.” So if we type “mudwort” into a normal type of search browser, it will tell you everything there is to know about a particular plant. If you do nonobvious relationships you type in “mudwort” and it gives you the nodal analysis chart—plant – country – etc.—until you have “Do you mean this individual who lives in this country?” With that individual you have a phone number, and that phone number feeds back up to that individual.

That nonobvious relationship software already exists. Jeff Jonas at IBM created this thing called NORA: NonObvious Relationship Analysis. He is an incredibly brilliant individual. He did most of the security for casinos. It’s interesting that the government may be able to take a lesson from casinos, because casinos have a blacklist of people with whom they cannot do gaming. If one of those people on the blacklist comes in and games in the casino, even if the casino didn’t know about it and was completely innocent, the casino loses its license. So from the time that person swipes the credit card to check into the casino, the system checks all those nonobvious relationships, because chances are that the person used an alias, or it’s the address of their mother’s distant cousin five times removed. It does all those nonobvious relationships, so that by the time that person gets the room key the casino knows if that person is on the gaming blacklist.

**Borg:** In your case, what data set are you pulling from?

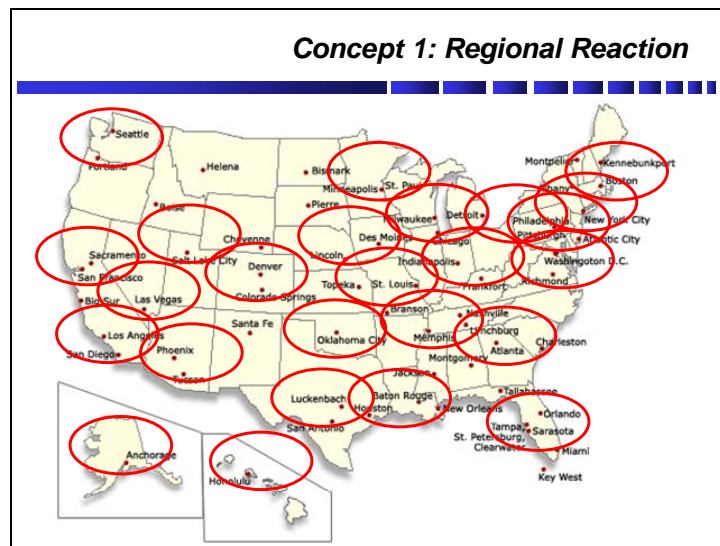
**Williams:** Initially it would just be all the intelligence databases. You might have one intelligence database that focuses on communications intercepts. Another one might focus on human intelligence. Another one might have signals intelligence. But within all these organizations there are stovepipes. For example, if you talk about terrorism most of them don’t talk among themselves as to what is Islamic terrorism and what is organized crime, or narco-terrorism. Now, Islamic terrorists might use organized crime to facilitate the movement of their

processes. The only way you're going to understand it is by being able to connect the dots among all those stovepipes and then going outside the borders of that intelligence agency and bringing in all the other dots.

So initially you want to do this just in intelligence. If you can protect the sources and methods, the sanctity of the data from the private sector, and many other things, and then eventually bring in the private sector data, you get high fidelity. Initially if you can just do it with U.S. intelligence that would be great.

Now, I've already talked a lot about this, but what about national security in 2010? How do we bring in the private sector to aid in national security? I'm just going to give you concepts that are on the street. They're not necessarily right, but these are what people are talking about at this level.

The regional reaction really hit the spotlight after we had Hurricanes Rita and Katrina, where all of these regions were taken out and we had a problem with response (**Figure 17**). The idea is: Why don't we build super-metropolitan nodes, where each node has an integral public-private sector entity, so in times of trouble that entity is already in existence and works like a war room. Everyone gets together and they're able to coordinate response. In fact, you have the equivalent of one of these right now in Boston: your Massachusetts Port Authority, under Admiral George Nakara. I would say it's one of the benchmark public-private partnering entities in the United States. Every morning around eight o'clock, at Logan International Airport, about fifty to sixty people congregate in one room—everyone from the state police to longshoremen—and they all discuss the threats of the day. Then they break up. It's a tremendous organization.



**Figure 17**

What is the problem of using this model for a national security-type architecture? Let me make things a little more simplistic (**Figure 18**). Let's say you have an earthquake in Los Angeles. You start mobilizing all your goods and services to deal with the earthquake. But it's an exceptionally lousy day, because a Category 5 hurricane hits the Cocoa Beach/Cape Kennedy

area, so you have to mobilize there, and then you have opportunistic terrorists who blow off a dirty bomb in Boston Harbor and also attack Chicago.

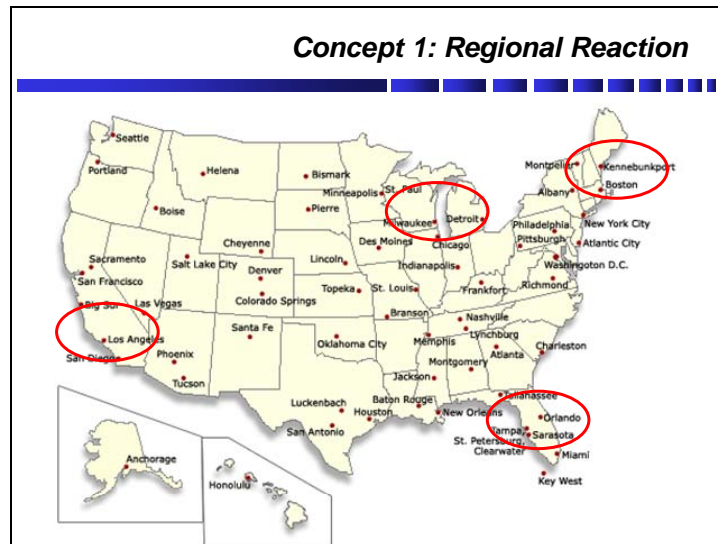


Figure 18

What takes priority? You have finite resources. Wal-Mart can only move to certain places. But you've got these regional nodes, and each one is saying "I want all the lumber and everything else coming to me." That node starts screaming all the way to Wal-Mart headquarters: "We need all your water.." Who takes the lead in this? You have chaos.

It's basically the problem we have fighting global terrorism under our present architecture (Figure 19). We have Southern Command, Northern Command, European Command, the soon-to-be Africa Command, Central Command, and Pacific Command. The terrorists understand our jurisdictions better than we do. You might have a situation that involves, say, just money. It might be narco-related money that goes from Northern Command down to Southern Command. From Southern Command it's moved through legitimate channels over to European Command. It's then laundered into Pacific Command and brought back over to Africa Command to get blood diamonds, which are sent over to Antwerp and sold. Who takes the lead? No one does, because it's in all of these commands. Each command will take the lead in its particular area. Which is the best area to hit? That's where your regional super-nodes will actually fall apart: in the face of separate cataclysmic events.

I don't think that's outside the realm of the possible. Terrorists aren't dumb. They've been watching; they can see what a couple of pounds of C-4 can do to the levees in New Orleans, so if there's another hurricane or another earthquake, it would be very easy just to escalate chaos by using C-4 on a levee. We have to be concerned about that.

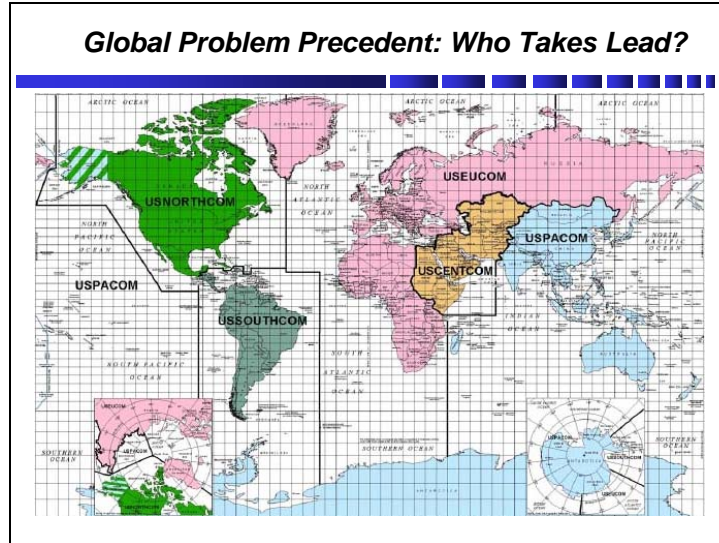


Figure 19

This is the second concept. This is what the private sector is tossing out. It's called the Federal Security Reserve System (Figure 20). We got a group of private sector executives together back in October 2003 and asked them to think about how they would structure an entity to be able to handle multiple domestic scenarios with a global scenario. It was actually a Wall Street banker who came up with this. He said, "Really what you're talking about is the Federal Reserve. Remember George Santayana's statement that 'Those who do not learn from history are doomed to repeat it'? Many times, these people learn from history and want to repeat it. As you describe terrorism, with its multiple dimensions and physical separation, basically what you're describing is 1903, with runs on banks. If there was panic and everyone made runs on one bank,

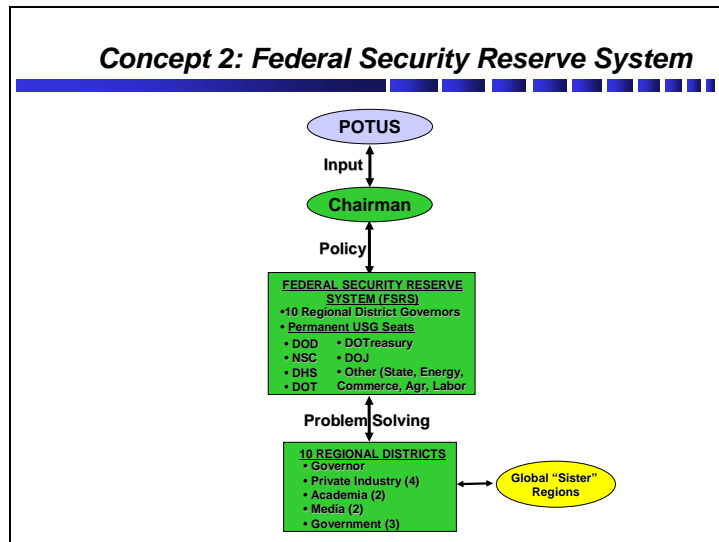
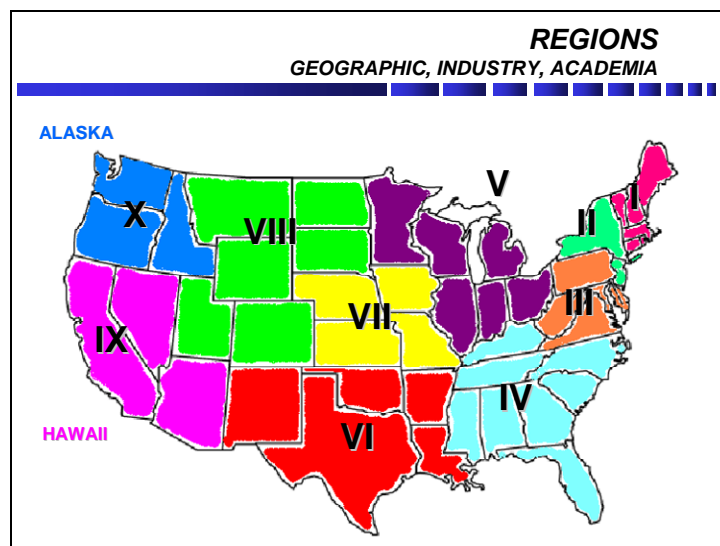


Figure 20

the bank didn't have enough money, which had to be shipped in from a local area, so the bank collapsed. There were hundreds, if not thousands, of different banks, and each bank printed its own currency." Imagine this! It was Go Fish: information saturation.

The solution was the Federal Reserve system, which we actually adapted from the UK. Under this scenario we used the FEMA [Federal Emergency Management Agency] model (**Figure 21**). These are the FEMA regions for response. When we started looking at it, we realized that each region has an industry where it has the preponderance in the United States. In the case of Region VI it's petroleum. Although there's petroleum on the West Coast and in Alaska, the preponderance of headquarters is in this area. So they would lead any effort that's required for petroleum. There's an emerging preponderant region and the actual one. Every region has an industry that represents not only the preponderance for the United States, but possibly also the preponderance for the globe.



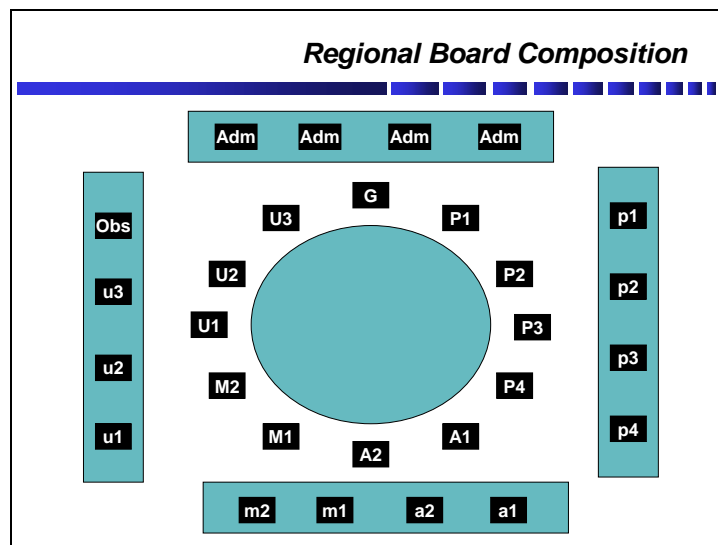
**Figure 21**

So we have these regional districts, much like the regional banks under the Federal Reserve (Figure 20). We took a page from chambers of commerce, and each region would be married up with a global sister region. So, in the case of New York, which is heavily into finance and shipping, we could marry it up with up with London, Bahrain, Tokyo, Singapore, and so on. Then, when we address a problem it's a global solution rather than a domestic one.

These regions are the equivalent of regional banks, which do their own demographics, their own analysis, and push it all up to the Federal Reserve Board. The board is composed of representatives of the U.S. government, but they're outnumbered by the private sector. It's a quasi-governmental organization. They look at it; they come up with policy, and they have accountability. Then it goes to a chairman who is selected by the president and confirmed by the Senate, and then you have the president of the United States.



This is the idea of the regional board (**Figure 22**), where you have priority 1 (P1)—private sector 1—which would be the predominant industry in this region. In Region VI, it was petroleum and energy, and the second one (P2) was telecommunications. They would be the rallying point for all the United States for that industry. P3 is the tertiary industry for that region. However, demographics change with time. P4 is the emerging industry for that region. A1 is academic institutions, such as Harvard, which is established physically in Region I but is global in reach. Then A2 would be a regional academic institution. Media 1 (M1) is a global media outlet for that region; M2 represents smaller media, and then government has three places. Along the side are the staffers, and their job is to research vulnerabilities and come up with solutions. In case of a crisis, you mobilize a regional war room. Behind this are about 130, if not more, global terrorism task forces that are embedded in every city.



**Figure 22**

**Borg:** Is the chairman then embedded at the NSC [National Security Council]?

**Williams:** It's much like Alan Greenspan was. A lot of people think the Federal Reserve is a government entity. It's not; it's a quasi-governmental entity. It gets its own money from membership and whatever. It operates outside the U.S. government but at the pleasure of the U.S. government. That is where they wanted to go.

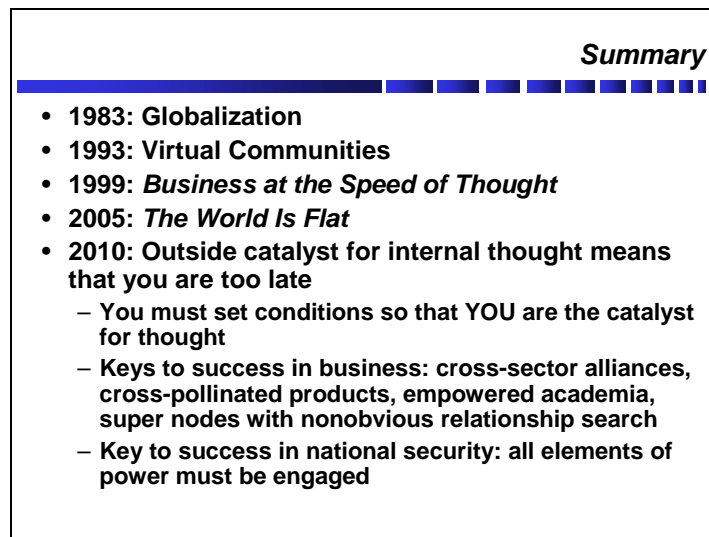
**Borg:** Taking a different cut on this, would it be beneficial to have a day-to-day effort at the NSC level where the interagency coordination could be reviewed and selected?

**Williams:** They would want to be aware of this, but they would not want to be embedded in it. The Federal Reserve isn't embedded in it. It's aware of everything, but the private sector wants the ability to take care of its own business. The interagency for the most part is a part of the board. They would have an entity on the board.

**Oettinger:** There's a complicated layer to this. The comptroller of the currency supervises the banks. The mission of supervision is different from what the Fed does, but my guess is that they talk to each other quite a bit, although it's not a formal relationship.

**Williams:** That's a good point. The scenario there is that the Federal Reserve walks in lockstep with Treasury. Just to let my mind run, it would be the same way here: the chairman would walk in lockstep with the head of the Homeland Security Council, because, in all honesty, if a problem happened, Frances Townsend would want to walk in lockstep for that purpose. It's just an idea; just a concept that's out there. This has to be created through legislative action. Unless the Congress actually does it, it looks like it won't happen.

Just to sum it all up, when I started looking at dates I realized that "globalization" as a term didn't actually start until 1983 (**Figure 23**). From 1983 to 1993, in ten years, we went from "globalization" to "virtual communities." Then, six years later, we had "business at the speed of thought"; I think it was Bill Gates who coined that. Then six years after that, we have "the world is flat," so you see that time is starting to compress. Now you have 2010, and in 2010 in business if you're waiting for an outside catalyst to generate internal thought, you're already too late. If I look at Tony and say "You know, that's a great idea" with a thirty-week turnover I'm too late. To be competitive in business you have to set the conditions so that you're the catalyst and everyone follows you.



**Figure 23**

The keys to success in business include cross-sector alliances. In national security all elements of power have to be engaged so that you have all elements of power sitting together around the table virtually. Again, you set the conditions: you say "In the next ten years I see we're going *here*, and this will open up this huge area for exploitation." Then you're already in front of the power curve.

**Oettinger:** Globalization goes centuries back, to the East India Trading Company and the founding of the American colonies, so I would scratch that date out. It's really the later ones that distinguish this era.

**Williams:** That's when the term was officially coined, although the concept goes way back.

I think that's it. If anyone has any questions I'll address those now.

**Student:** Why is this center located within the Department of Defense? You clearly need an ongoing relationship with the U.S. business community, but why the DoD? Why not DHS or ...?

**Williams:** Everyone asks that question. First I'll go over why it shouldn't be in certain areas, and then the answer to why it's in the DoD will be very simplistic. It shouldn't be in DHS. They should have a piece of it. Remember, DHS focuses from the borders in. Most organizations—the Department of Treasury, the Department of State—have a public-private entity, but it's specifically designed for their niche. For example, the Department of the Treasury they has one, but it's specifically designed for terrorism in connection with finance issues. Our particular center is designed to look across all parts of the spectrum. DHS would be the only other place you could put it. There'd be a piece that you'd want to put in the FBI [Federal Bureau of Investigation], which is part of the Department of Justice, but really the lion's share would be in DHS.

The reason why it's in the DoD is because we're the ones who thought of it. It's as simplistic as that. It started in the DoD. We briefed it up to Secretary Rumsfeld. We actually tried to get rid of it. We tried to give it to the NSC. That's really where it should be, so you can look across all interagencies and be able to move freely. But the staff at the NSC is incredibly small. They came to us and said "We can't accept it. We don't have any staff. Will you do it? You have the trusted relationships that are already mature. Keep it." That's as simplistic as it was. The private sector, frankly, would rather have it not in the DoD. They would rather have it right under the president. But their opinion is that if it's not in the DoD they can't think of anywhere else it should be.

**Student:** How about the NCTC [National Counterterrorism Center]? Obviously, the intelligence agencies have a certain aspect of it.

**Williams:** Your question actually gives away the answer. Why not the NCTC? What about pandemic influenza? We've worked with the NCTC through the JTF-CT [Joint Task Force-Counterterrorism]; however, the already demonstrated potential of this organization is greater than just terrorism. That's why they changed the name from Partnership to Defeat Terrorism to The Partnership Group, because we've been working on everything from "Is it good to release an anti-Islamic cartoon?" to "How do you detect pandemic influenza faster?" You're harnessing all elements of power to address difficult problems rather than difficult terrorism-related problems. So that's why it's not in NCTC, although we do work with them. They also have a public-private partnering entity that they're developing.

**Student:** When you talked about the work on the ground—what the foot soldiers, if you will, in your group do—I'm immediately reminded of case officers: it's essentially building relationships. It sounds a little manipulative, but it's an aspect of it. Is there any particular training for the

people who actually do this type of work? Do you also run into problems with the whole PCS [permanent change of station] cycle of commitment for a couple of years?

**Williams:** The PCS cycle was a problem. Liz,<sup>6</sup> for example, is actually retired military who is now a government civilian. A government civilian brings the continuity. I'm active duty, but I'm coming to the end because I'm coming up on retirement. You can't afford to have those nodes go away, so one of the initial things directed at that January meeting in 2005 was that it had to be run by a civilian just because of that factor.

You also asked "What about the individuals who are hired? What is their experience, and what is the training?" The bottom line is that you're not going to get hired as a subject matter expert unless you have a demonstrated history as an expert in that particular sector. Our transportation subject matter expert, for example, has almost thirty years of demonstrated success as a maritime expert. They're all Ph.D.-level individuals.

**Student:** Congratulations for getting them out to Omaha!

**Williams:** It's called capitalism.

**Durham-Ruiz:** Yes, it is, but I'll tell you: when the center was set up, just the idea of the center and what we're doing now meant that a lot of people have come knocking on our door and asked "How do I get to work out there? This is a neat idea." People whom we've briefed can see the utility of the idea, but they always turn their head sideways and ask "How are you really going to do that?" But they would like to come and be a part of it.

**Williams:** What Liz says is correct. There's a phenomenon out there. We believe that everyone is motivated by money, but if you look at your Google models and everything else people are motivated by the challenge. You can't pay them peanuts, but if you pay them a good salary and you can guarantee that every day is going to be a challenge you're going to attract people. Suppose you're the maritime expert and you've worked your whole life doing maritime, and all of a sudden you find out you're going to speak with the chairman of Maersk Shipping. That is a huge rush! So that gets people out there.

**Student:** I guess you've kind of addressed this in your answer—that there's this additional psychological incentive—but to get specialists in certain fields I would imagine that you might need to go beyond your general GS [Government Service] pay grade. Do you have special budgetary authority to do so?

**Williams:** As of now, we haven't even had to go into that area. Remember, the subject matter experts are not going to be the question answerers: they're going to be the conduits. The private sector calls them "librarians." They're the conduits to the individuals who are so saturated they can't come to Omaha: the chairmen, the CEOs. There's an effort underway in all the U.S. DoD commands called the Joint Interagency Coordination Group. It's an interagency group that is resident in the headquarters: they have a Treasury guy, an FBI guy, and so forth. What we found

---

<sup>6</sup> Elizabeth Durham-Ruiz is Lead, Partnership Group, GISC, STRATCOM.

is that the people they send to these groups are people whom for the most part they can release to go to those groups. The individual you need in a crisis is the one who is only one deep: who is so saturated that he's not in any group, and if you get him on the phone you might only have fifteen minutes with him. So we hire our subject matter experts for their expertise, because they know how to phrase a question, how to get access to these individuals, how to get the answer very rapidly and then hang up, and then they can metabolize what they got into something we can understand.

**Student:** When you're dealing with the private sector, depending on the challenge the person talking with the subject matter expert, the CEO in the actual company, might gain some sort of insight that might help his business. Obviously, there's the incentive of trying to help your country, but do you see that as another motivation for participation?

My second question is a little more light-hearted: why are there no windows in your building?

**Williams:** I'll answer the second question first. This was built by a very visionary multibillionaire, with something much like the Kevin Costner mentality of "If we build it they will come." He built this building to house classified defense contractors. On the other side of the parking lot is something called an incubation center for technology. His idea was "If I build this for a classified organization, then defense contractors will come."

Second, we have a lot of tornadoes in Nebraska. He built this thing to withstand almost a direct hit from a tornado. He's an interesting gentleman, and he knows how to build things to last. The walls are about twenty-four-inch steel-reinforced concrete. It is basically a bunker. We had a level 1 tornado that went through the parking lot right after we were stood up. It's an amazing place! I was able to stand at the door and just watch the tornado come by. All the people from the incubation center were running out of their building like ants and coming to our building.

On your first question, that is always a problem: that an individual who is consumed by greed of some kind might either give you faulty information to manipulate an action or take what you're saying to be used for gain. First of all, I don't think there's anything we can do to stop giving out information that someone can use. The alternative is not to do anything and just hope an attack doesn't happen. Hope is not a course of action.

So the first piece of the question is: If I have information of an impending attack, do I tell him about it, hoping that he doesn't do insider trading, or do I just sit on it, because I don't want any of that to happen? The bottom line is that the people in this group are world-renowned experts in their field: chairmen and CEOs of major corporations. Their whole livelihood is based on being the figureheads for that sector. If they were to do something that would give them gain, everyone around them, first of all, would detect it, and basically they would lose their standing. That takes care of their using something we give them for gain. Also, we monitor them.

The second piece is: What about their giving us a piece of information to manipulate an action? We don't take anything we get as gospel. We corroborate it. Remember the "Go Fish" scenario. If the chairman of some corporation calls me and says "We just had a strange event happen here" the first thing I would do is ask "Did you notify the FBI or whomever?" The second

thing would be to ask “What is your action? What happened?” When he tells me, and I know that if it’s passed forward it would elicit some action from the U.S. government somehow, we then go back to the intelligence apparatus and ask “Do you have something that can corroborate this?” They may or may not. Usually they do. Then we’ll also go to a competitor and ask “Have you heard about such-and such?” or “Is this possible?” We have to get corroboration.

If it is a very trusted source, we will still send it forward, but we will caveat it out the wazoo: “This is from one source. We could not corroborate it, but because of its serious nature you need to be aware of it.” So that’s how we do it.

**Student:** My greatest question/concern is that if we’re focusing on the nature of the enemy and their financial system, they work through these hawalas, couriers, gold transactions, and all that. If we’re tapping Bill Gates, he might be familiar with how to build a Fortune 500 company, but are we getting the right people who understand how markets in the Middle East work and how they’re moving money?

**Williams:** I think you’re putting a couple of things together. We deal with all global infra-structures, so we would not go to Bill Gates to try to understand about hawalas. We would go to Bill Gates if we had to understand about information technology of some kind. With hawalas what we would do is go to academia, because you’re talking about a cultural aspect. Even with hawalas we’d have one individual calling someone in another country and brokering trust. Can we do anything against hawalas? No. The black market peso exchange in South America is along the same line, but if we start locking hawalas down they’re going to go to something else. Another thing now is cell phone cards. which they’re using as a commodity, so we would go to the sector that could give the insight.

For hawalas we would probably go to two places. We might go to Citigroup, because they do sharia banking. We would probably go to academia, which has embedded individuals in these countries that actually operate with hawalas. If you have something like a courier, hawalas, black market peso exchange, hindies, all of those things, you’re talking about more of the socio-economic piece than you are a technology piece, so you go to the expert. Sometimes finding the expert is one of the hardest pieces.

**Borg:** Is the human in this the critical node? In other words, when a problem comes in, do you have to have the requisite knowledge to know which area to tap? Is it academia, or is it a technology sector?

**Williams:** That is why we have the subject matter experts. The way it was done previously, message traffic would come in and you’d have an intelligence analyst reading it. That analyst had probably been looking at that message traffic for thirty years. He’d say “I don’t see any of the buzzwords that tell me this is important. Or, let’s see: this one says ‘uranium.’ Oh, uranium! That’s critical.” What we found is that the human in the loop has to be able to look at that intelligence traffic and say “Hmmm, that sounds like shipping.” “That’s a sixteen-digit number; okay, that’s a SWIFT [Society for Worldwide Interbank Financial Transfers] transaction number.” They look at it through their own lens, so they can say “That traffic is talking about a financial transaction,” and then go out from there.

**Borg:** So if I'm understanding it correctly, to make sure that you interrogate that information appropriately you're having subject matter experts from across the board look at every piece of intelligence that comes in?

**Williams:** You can't. There's only one solution to that, and a couple of intelligence community organizations and national labs are getting with industry subject-matter experts to help them create keywords and taxonomies pertinent to their industry, like taxonomies for fraud and credit cards. That's the only way to do it at that level, because with the volume of the intelligence traffic it's basically "garbage in, garbage out." You have to have the right keywords to put in to flag something. All we can do is train some intelligence analysts to look at traffic, but it's only a minute piece. When we get tasked, the task might be for a particular action, but when all our subject matter experts look at it they may say "That action won't work. You ought to go over *here*." That's the best we can do with the staff we have.

**Oettinger:** Can you go back to that slide about the nature of the questions (Figure 4)? You point that out as a solution, but ultimately what you're describing there is the search for knowledge and the scientific enterprise and so on. It seems to me that the customer of intelligence ultimately has to realize that there are areas that are unknown and unknowable on the timescale of the phenomenon under consideration. You don't get at penicillin by saying "I'm going to discover an antibiotic." Instead, you are smart enough that when the accident happens you say "What's the question that would fit this?" You find the nonobvious relationship between this mold and a disease, and lo and behold you have penicillin. But there's no way that's programmed.

It seems to me that one of the problems the intelligence community faces is misplaced expectations that somehow one can always figure out what the right question is and find the nonobvious relationships. You may have to wait a week or a millennium for that to happen. Putting it that way risks perhaps setting up dangerous and unfulfillable expectations. I would urge you to find another way of phrasing that, because it would be egregious for something that is mission impossible.

**Williams:** I agree up to a point: it's mission impossible, and maybe I need different words, but it's the path they have to travel, and it's not there. We found, for example, that when you talk about terrorism as a whole, or about multiple aliases and how the architecture is set up, it's going to have to be done through nonobvious relationships.

**Oettinger:** There are ways of putting yourself in the path of serendipity, but the serendipity is still there. So it would seem to be worthwhile to inject that element.

**Durham-Ruiz:** The timing is very important for nonobvious relationships. If you address the topic today, and you address it six months from now, your answer may be more acceptable and you may find more of the experts who have the right answer. These are some of the issues that we struggle with, because we have to provide an answer very quickly. We may have an opportunity to address it later, but timing is everything.

**Oettinger:** There has to be a recognition that by stating it so starkly you're inviting the "why couldn't you connect the dots?" question, and the answer is that foresight is harder to come by than hindsight.

**Student:** On one of your slides you talked about FOIA and FACA. When you were here last year you mentioned setting up an FFRDC [Federally Funded Research and Development Center] structure to get around that. Could you talk about that a bit?

**Williams:** If you go back to Figure 9, here's the legal problem. We were standing up the GISC, and the real problem came with staffing. If we in the DoD went out and hired all of these experts, and they came in as U.S. government employees, then any information given to them—the subject matter experts—would be subject to the FOIA. Granted, we could probably beat it, but it's still under the FOIA.

So then the thought was “What if all of these sectors would loan us an individual: a person they would identify who would sit there in the facility? We would not pay them. They would not be our employees, so they would be able to take all this proprietary information.” But what happens when all these individuals get together and form a consensus? For instance, they say “We think you should move your carrier group *here*.” That gets close to the FACA. Think of Vice President Cheney's energy commission. According to the FACA, the private sector cannot come together to form a consensus and give that consensus to the U.S. government in the form of a recommendation.

So we had a problem. What should we do? We found the only solution was to have employees from FFRDCs, such as RAND, IDA [Institute for Defense Analyses], and CNA [Center for Naval Analyses], because as FFRDCs they're allowed to swim in both waters. They have memoranda of understanding and agreement where they can take proprietary information and they're absolved from the FOIA. They can also sit in on government discussions and give consensus, and they're absolved from all that FACA stuff.

So the idea was that in areas where we may get that type of information we were going to hire FFRDCs. Initially the predominant one was in finance, so we had a finance FFRDC individual. We no longer have any FFRDC individuals, because at this stage, with being in Pillar 1, we're not really getting any of that privacy-related information. If it comes down to the point where we start getting that type of information then we'll go out and get the FFRDCs.

**Oettinger:** At the risk of underscoring the obvious, let me just underscore for the class that what you're looking at here is in many ways the central detail of a masterpiece that these guys have accomplished. These are points where there are difficulties that Darryl seems to have overcome in an extraordinarily inventive and effective manner.

By contrast, you mentioned John Poindexter and the Total Information Awareness project, which was a classic example of how to do everything here totally wrong. Mistake number one was to talk about “total information awareness” as a goal, which is technically absurd, conceptually absurd, and overreaching to the *n*th degree. That made it vulnerable to attacks from peers in the technical community. That in a sense was a bit of overenthusiasm by John Poindexter. John is one of the nicest people in the world, so it's hard to imagine that he's a convicted felon. He happens to have been pardoned, but if you put a pardoned convicted felon in charge of a project that claims—although falsely and overreaching—that it will organize every piece of data about everyone in the universe, including your own happenings every five seconds, somebody is bound to get exercised about it. There isn't an item here on the slide that was sensibly dealt with



in that project, so it eventually exploded. That is too bad, because hidden under the verbiage and under the felony, et cetera, there were some good ideas. But there was neglect of the most elementary concern over the political, legal, and organizational issues, and the focus was almost exclusively on “Hey, technology can solve this!”

What is so elegant about this solution is that there’s an element of technology, but there’s a sensible recognition that the best tools in the hands of nonfunctional organizations, and without the proper legal framework, aren’t going to do anything worthwhile for you. That’s what this slide shows, so if you take nothing else away from the briefing you should remember that set of items, which most people don’t understand.

**Student:** If your subject matter experts work in a Fortune 100 company I suppose they’d be a little worried about its getting out into the newspapers that they worked through this process. People would assume that they must have shared private information. Is there that concern among these participants about negative repercussions if this came out?

**Williams:** For the most part, no. There are a few corporations that do not want to be identified as supporting this effort. We don’t have an electronic area that has any of those individuals attached. In fact, it’s basically just a few people who are aware of it. For the most part, as long as the target is global terrorism or hard problems of the U.S. government we have not had any problems with any company’s saying that it pushed their risk too high because they’re working in other countries. Now, if this were absorbed into an intelligence organization, and it got out in *The New York Times* or wherever else that companies A, B, and C are giving information to an intelligence organization, all of a sudden their operational risk would go through the roof. But if it gets released that companies A, B, and C are supporting an effort to combat global terrorism, especially to combat global terrorism’s exploitation of their particular sector, they’re looked on as champions. It actually gets on their ledger as goodwill. That’s why it’s very important to keep this neutral.

**Oettinger:** I think there’s another element that might be worth underscoring. It’s the expertise that you’re going after. You’re not asking for proprietary information: you’re asking for stuff that is unknown in the government and may be unknown in this classroom but is daily bread for the people doing whatever it is they’re doing. For the information sources in many instances it’s painfully obvious, and nonproprietary, and public within their sphere. Again, to me it’s one of the elegant aspects of this. There may be stuff that is proprietary, but you can go a long way by going to people who practice things every day and therefore have knowledge that to them is second nature and public but happens to be extraordinarily precious to someone who is not initiated into the club. But you wouldn’t know it, because you’re sitting in your office in Omaha and have no idea what’s happening in Delft or Bahrain.

**Durham-Ruiz:** As an example, in one instance we had a question posed to us “How would you stop a ship that might be carrying a cargo that you didn’t want to dock at a particular port?” We called up one of our partners in the shipping industry, and he said “Well, that’s obvious. You just get out there and talk to the pilot, and the pilot will stop the ship.” We didn’t know anything about pilots or ships or port operations or anything like that. But it was just a simple process kind of

question, with no specifics about the instance. It's just a process kind of thing that is obvious to those folks but is not obvious to us in this particular section of the DoD. So it was very helpful.

**Oettinger:** Lest this seem to you excessively simple minded, let me contrast it for you with the normal, routine process a three-letter agency, where a technical question might arise and be passed to someone who is a chief of station—whatever the agency calls its station chiefs—and then it's passed to someone who goes and talks to someone, but none of them has any subject matter expertise. Then it goes back up the chain and the information gets distorted by several layers. By now three months have passed. You've all played the children's game where you have a question and it's passed around and at the other end it bears no resemblance to the original question. That describes an ordinary intelligence agency process. So the procedure that's being described here is rather unorthodox, and therefore gets competing agencies riled up.

**Williams:** That's mild!

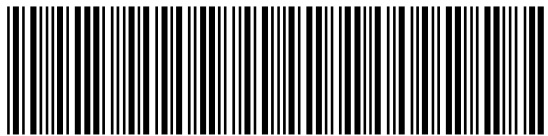
**Oettinger:** You don't necessarily get rewarded for doing something sensible.

**Williams:** I guess I've worn them out.

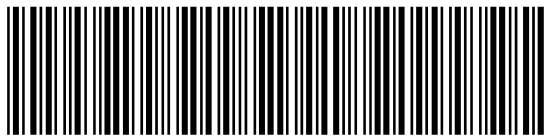
**Oettinger:** Darryl, thank you very much for another excellent presentation. Here's a small token of our large appreciation for you, and an even smaller token for Liz.

### Acronyms

CDC	Centers for Disease Control and Prevention
CEO	chief executive officer
DHS	Department of Homeland Security
DoD	Department of Defense
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
GISC	Global Innovation and Strategy Center
I <sup>4</sup>	ideas, innovation, implementation, and imitation
NCTC	National Counterterrorism Center
NSC	National Security Council
PCS	permanent change of station
STRATCOM	U.S. Strategic Command
UK	United Kingdom



INCSEMINAR2007



ISBN 1-879716-98-4