INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Risk Management in the Department of Defense
Carol A. Haave

Guest Presentations, Spring 2004
Carol A. Haave, Mark M. Lowenthal, Robert B. Murrett, John C. Gannon, Joan A. Dempsey, Gregory J. Rattray, Robert Liscouski, Arthur K. Cebrowski, Aris Pappas

May 2004

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.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN I-879716-89-5 **I-04-1**

May 2004

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp. (Japan)
PDS Consulting
PetaData Holdings, Ltd.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Strategy Assistance Services
TOR LLC
TransMedia Exchange
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Verizon

Risk Management in the Department of Defense

Carol A. Haave

February 19, 2004

Carol A. Haave is deputy under secretary of defense for counter-intelligence and security. In this position she provides policy, technical, programmatic, and department-wide oversight, coordination, and integration support to the under secretary of defense for intelligence on all aspects and matters related to Department of Defense (DOD) counterintelligence, security, and risk management. From November 2001 until assuming her current job, she was deputy assistant secretary of defense for security and information operations. Previously she was president of Sullivan Haave Associates, Inc., a woman-owned company operating solely on behalf of the DOD to facilitate the transition of advanced technologies into military operations. She began her career by enlisting in the U.S. Army, earning a commission, and advancing to operations as an airborne-qualified military police officer. In 1978, she became a special investigator for Summa Corporation and conducted background, gaming, and organized crime investigations in cooperation with local law enforcement, state gaming control officials, and the Federal Bureau of Investigation (FBI). From 1985 through 2001 she consulted for the U.S. Congress, Defense Advanced Research Projects Agency (DARPA), National Imagery and Mapping Agency, and other government agencies. Among other assignments, she was a team leader for the House Appropriations Committee's Surveys and Investigations Study on Global Command, Control, and Communications Systems across the military services and a member of the National Defense Panel staff that investigated alternative military force structures in 1997. She received a bachelor of arts in sociology from Stetson University and a master of arts in human resources management from Pepperdine University.

Oettinger: Let me briefly introduce our speaker today, Carol Haave. You have seen her biography. She expects this to proceed as a conversation rather than as a lecture, so don't let me down. Probe and ask questions. We are delighted to have Carol with us.

Haave: Thank you. I have a prepared speech. How long is this class?

I have a very eclectic background. I've worked in the Congress, in the executive branch, and for industry, and I have both intelligence and operations experience. In all the time I've spent in the Defense Department in various capacities I have never learned to do PowerPoint. I don't

talk to PowerPoint, so I know you'll be distressed and disappointed to know that there will be no slides out of this conversation.

I think it's fabulous that you are here in this program, because you represent the future and there are a number of things in this twenty-first century that probably most of you are more comfortable with than those of my generation or those who are older. That is not to say that Professor Oettinger isn't perfectly up to speed on the whole electronic environment that we live in today.

We are in an exciting time in the intelligence community and in the DOD. We are undergoing what we believe to be a transformation. We used to have a term, "revolution in military affairs." The truth is that we've talked about this revolution for a long period of time, but I would argue that we have not actually achieved it yet, because the revolution in military affairs, in my estimation, is about information, and we can barely spell it. I don't think we have come to harness the power of information, and therefore we have not harnessed what may be the potential of the intelligence community. We need to find new ways of doing that.

What you see in the DOD is a philosophical discussion about the intelligence community. What is its proper role? What should its mission, tasks, and activities be, in support of what, and in relationship to what? How do we achieve the horizontal integration that we are so desirous of? What aspects of our intelligence capabilities, our DOD, and the elements of political power—political, economic, military, et cetera—support our strategy?

I represent the under secretary of defense for intelligence. I am the deputy under secretary for counterintelligence and security. Until the reorganization that took place six to eight months ago, I also had critical infrastructure protection, information assurance, and information operations in my portfolio.

As you know, the world has changed since 9/11, so counterintelligence and security, and intelligence in general, are very exciting topics at this time. They are exciting for a number of reasons. One is that we will never be able to protect ourselves against any eventuality or potentiality that may happen. There isn't enough money in the U.S. Treasury to do that. After Khobar Towers, which you may remember—the 1996 bombing of the building in which nineteen people were killed—there was great emphasis on protection of our assets: infrastructure, buildings, personnel, et cetera. We call that force protection today.

The truth is that we write policy so that one size fits all: in other words, everybody has to abide by it equally. It doesn't really account for the fact that—as politically incorrect as this may be—some things may be more important than others. There may be some military installations that are more important to us than others. There may be specific types of military capabilities that are more important to us than others, and we may choose to protect them first, or in some priority fashion.

What that drives us to is wanting to get to a risk strategy in the department, because what's happened with "one size fits all" is that we are risk averse and risk avoidant, and we can't get there from here. Khobar Towers is a beautiful example of this. The one-star general who was in charge of the installation at the time basically was retired as a result of the bombing. I think that sent a message to the military leadership, not only in the Air Force but also in the other services,

that what happened to that person who was forced to retire was not going to happen to them. So there were Navy captains who would not let their sailors off the ship in port, because nothing good was going to come from that. They went by the book in terms of asking for—and I say this euphemistically—the gold-plated faucets, the velvet drapes, and the marble fireplaces. They were absolutely going to request—in writing, through the chain of command—every single item they could think of that was required for force protection or was documented, because they wanted the leadership of the DOD to tell them, in writing, "No, we can't provide you that. There are not enough resources."

That mindset drives you to want to create a risk strategy, which we are doing right now. We talk a lot about threat. For me, walking down the stairs in high heels is a threat, because the chances—probably not too remote—are that I might fall. I did that once. People actually laughed. People's reactions when something like that happens are really interesting. You fall down the stairs; clearly you could kill yourself, you certainly may be hurt, and people laugh. That's a sort of fear-based reaction.

Oettinger: Before you go on, I want to seize occasional opportunities to relate what a speaker is saying to readings. This question of over-compensating and taking the wrong message from the guy who retired and so on is a very critical problem. We're obviously not going to be able to plumb its depths during this semester, but keep Carol's remarks in mind when you get around to reading Scott Snook's book,[1] because that's what it's all about. It has to do with the downing of the Black Hawks in northern Iraq by U.S. fighter planes, but the issues of, first, how you prevent that sensibly, and second, what do you do after the fact in terms of sending the right message to future fighter pilots or helicopter drivers or whomever is nontrivial. Scott Snook's book is all about what was here a passing remark.

Student: Do you mind if we interrupt you with questions?

Haave: Absolutely not. In fact, it's easier for me if it's interactive, because that way you get out of it what you need, and I actually learn that way. So please interrupt.

Student: You talked about horizontal integration. In your opinion, are we asking too much of our intelligence community, and of the DOD, when we ask them to integrate horizontally? Sociologically, when you look at the bureaucracy, it is structured more to deal with the efficiencies of the things we know about. I'm sure everyone has heard the Rumsfeld statement about the "unknown unknowns." How do we get to a more adaptive organization that focuses more on finding the unknown unknowns than on dealing efficiently with something that we know we don't know, but at least we know that?

Horizontal integration also runs up against that bureaucratic tendency to keep secrets, known as compartmentalization. How are we going to integrate so that the means of keeping something secret don't become the ends of keeping something secret for secrecy's sake? You can look at parallels in history. For instance, in World War II the British and American governments would probably have sacrificed an entire division before they would have let the Germans know

[1]Scott A. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq* (Princeton: Princeton University Press, 2000).

that we had broken the Ultra code. So, how do you walk that fine line between maintaining something that's absolutely critical for our defense as secret and letting out that we have this capacity to sense something or collect something if that could save American lives? How do we negotiate that fine balance and maybe conclude that the lives aren't worth giving up that secret?

Haave: We are in the throes of having that debate right now. Let me give you my bias on this. I have spent my entire career trying to make life better for those who are most at risk, and by that I mean those who are in harm's way. The further away from the Pentagon you are, the more inclined I am to support you. That just happens to be how I look at the world. So, as we look at horizontal integration, I think we first need to define it, and I'm not sure that we've defined it in a way that everybody agrees on or understands. It means different things to different people.

I think we are trying to break down what we call the "stovepipes" of intelligence. Whether it's signals intelligence, human intelligence [HUMINT], imagery intelligence, or whatever, we have created these functional hierarchies, if you will, whose power would be best achieved if they were horizontally integrated. Some of that can be done fairly easily, and what you see in the DOD is that we in fact horizontally integrate our collateral information to the extent that we can.

Where we have some debate is about how much of the intelligence information is going to be included in that. The way we're structured today, the owner of the intelligence determines who has a need to know. In some cases, that organization may not be best equipped to understand the end use of that information.

The way that I look at it is that we have to come to an agreement about what we are trying to do. For example, if we want agencies to share their information and recognize that information is power, we have to assure them that the people who have access to it have a need for it, are properly cleared, are authenticated, know what to do with the information, are not going to do something untoward with it, et cetera. There are technologies today that will allow us to do that. We have chosen not to implement those technologies. A statement I hear a lot is "Policy should drive technology." We should write the policy and then the technology that implements it should be brought forward. I have to tell you that I disagree with that, and I've come to that conclusion over several years of doing technology transition in the department. If there is an organization or an agency that does not want to do something, it will write policy that will exceed the limits of technology, and we will not get there.

At least in the DOD there is an initiative on horizontal integration going on right now, and I have said: "Bring me your technology solutions to these problems. How are we going to do assurance? How are we going to certify need to know? How do we ensure that originator-controlled information does not exclude the people who have rightful use of it in an electronic environment? How do we ensure that the people who have access to the information are doing the proper things with it?"

If you ask me what keeps me awake at night, it's the privileged, trusted insider. That's where the most damage can be done. How do you ensure that people are behaving well on the network and with information to which they are given access? Until we can convince the community that we have a way to do that, they will be reluctant to share that information.

Student: One of our readings for today was an article about the CIA [Central Intelligence Agency] and how they feel that informing analysts of where intelligence information came from—who the sources are—is not always important.[2] How does the DOD feel about that, and how would that affect how intelligence is analyzed?

Haave: I think a process can be created whereby sources and methods are extracted from the information and a degree of confidence is given to the information. The way you will get there from here is to "crawl before you run" and have people actually making that evaluation manually, if you will, until the users get comfortable with the methodology by which you're going to do it. To the extent that you can mask information in an all-source environment, where all the functional disciplines come together and that information is analyzed and processed, you have more of an ability to protect those sources and methods.

Those are all things that we're working through, and in fact we do some amount of horizontal integration today. We see it in some of the disciplines. Depending what the situation is, we actually have a high degree of it in some areas and not enough in others. Where it makes the most difference is operationally. We do the best that we can, and I think it works fairly well in an operational environment, because at that point people are at risk and the walls sort of come down, especially with perishable data.

I think we have the greatest potential in the analysis area. Right now, we need to think about how to do competitive analysis. How do we better take advantage of resources that traditionally we have not taken advantage of in the community?

For example, I have a sociology background. In the fields of intelligence and information, I am very interested in having views from social and cultural anthropologists, behavioralists, psychologists, historians, and academics. There's a plethora of folks out there with different perspectives, and my personal belief is that the more perspectives you can bring to a problem, the better the answer will be in the end. So, at some point, when you're talking about horizontal integration and sharing, you have to get to a community of interest. You have to define that community of interest, you have to have a governance strategy about how that community is going to behave and what the rules are, and then you have to monitor its behavior. To the extent that you can conduct some of those experiments in a way that satisfies people's concerns, you will move forward. But what I see taking place now are conversations at different levels, using different terminology with different meanings, so we're not really able to close on it.

I might add that all of this is steeped in law. You have the National Security Act of 1947 and Executive Order 12333.[3] A number of other things come into play when you're talking about this issue.

Oettinger: I'm glad you said that, because without disagreeing with anything you said, I want to add the importance of these legal structures. You talk about different communities of interest. If

---

[2]See Richard L. Russell, "Intelligence Failures," *Policy Review* 123, February–March 2004, [On-line]. URL: http://www.policyreview.org/feb04/russell.html (Accessed on 10 May 2004.)

[3]The White House, Executive Order 12333, "United States Intelligence Activities" 4 December 1981, [On-line]. URL: http://www.cia.gov/cia/information/eo12333.html (Accessed on 10 May 2004.)

somebody's career is wedded to a particular stovepipe or whatever, that person will at best pay lip service to another community, and with good reason. Prior to the passage of the Goldwater–Nichols Act of 1986, people in one service would do purple service—that is, joint service—only at the risk of having their careers shot down. That changed somewhat after the passage of Goldwater–Nichols. There is no comparable instrument within the intelligence community, so people who want to further their careers had better hew the line to their particular specialty and not engage in excessive ecumenical shenanigans of the type that Carol is describing. So, without making that organic change, you will only get lip service.

Haave: That's a huge point. The question becomes: how do you incentivize good behavior? I say you have to reward good behavior and punish bad behavior.

Let's just take a hypothetical that reflects the way we're structured today. Agency X captures Osama bin Laden. Agency X gets all the credit for that, probably gets plussed up in dollars, et cetera, but that does not lend itself to horizontal integration and sharing. What you have to do is incentivize the federation. If you want to make horizontal integration work, you have to find incentives for all of the organizations to want to participate.

When I put together big programs, for example, I have a vision of what the future may look like, and I realize that my vision will probably not come true in this go-around, if you will. So I go to all the organizations that are going to participate and I ask them, "What do you need to get out of this in order to play nicely with others?" They'll say, "Well, you know, my director really wants to move in *this* direction," or "We need to get *this*," or "We need *this* amount of dollars," or "We need *these* kinds of people." I collect all of the input. My theory is that everybody should win something of importance, but everybody can't win everything they want. My vision of the future is modified by the reality of the participants and the process. Is it as far as I want to go? Probably not. Does it get us leaps ahead? Possibly. It certainly takes us steps ahead.

You have to incentivize people to do the things you need them to do, and you have to be creative in how you do it. For example, I'm a change agent. I have a list of people in the DOD whom I consider also to be change agents. When I want to do something in the department in terms of transition or transformation, I structure experiments or demonstrations or operational capabilities that will allow me to take advantage of those change agents and to demonstrate that a capability is, in fact, viable and will do the things it needs to do.

Student: It could be that another couple of spectacular terrorist attacks against us would provide just this incentive externally rather than internally. There was a greater sense of collaboration in the immediate aftermath of 9/11. It has sort of rebounded from there, but it did begin to break down the barriers.

Haave: We have made some strides. You saw with the Patriot Act that law enforcement information is now more readily available for analysis than it was in the past. External events are very much catalysts in moving in the directions that we want. But the bureaucracy is typically not a learning organization. Just as force protection is the DOD's number one mission, the number one mission of the bureaucracy is to survive. It will do everything it can to do that.

Oettinger: Just as a gloss on force protection, I believe that when Carol says that she means protection of the military infrastructure, not necessarily the civilian infrastructure. You have to be very careful about how you interpret the terms. I stress that, because in terms of the boundaries between what is the military and what is the Department of Homeland Security and who does what where there are a lot of unresolved issues. This is something to keep in mind.

Student: Could you talk a little bit about counterintelligence with regard to the asymmetric threat? I'm wondering if that trusted insider who keeps you awake is still the same kind of problem. We have trouble penetrating Al Qaeda, but they probably have the same kind of trouble. Furthermore, they really don't need to penetrate the government to do a lot of damage. A nation-state has to get inside our command and control, but a terrorist organization can go around it. Is there the same counterintelligence threat that there was before?

Haave: Thank you for bringing me back to threats, because I want to get back to risk strategy. Threats come in all shapes and sizes. From a counterintelligence standpoint, another one of those things that keeps me awake at night is that we are a very open society that is easily exploited. We have a culture that is very optimistic, very positive, and very trusting.

I think one of the biggest threats to this government is what I will call the technology drain. We devote a lot of resources to technology: science and technology, research and development. Because of the openness of our society that technology becomes available to lots of other people, which therefore erodes not only our technology advantage but also our economic advantage.

The protection of military capability technology is very important. Yet almost every day you can pick up the paper and read that someone has leaked some classified information (that's another one of my pet peeves). I don't know how to protect against stupid behavior. I think the biggest bang for the buck, frankly, is in security education and training and awareness: having an understanding of what is classified and what is not, which people should know from going through the process of obtaining their security clearances and working on programs.

Student: That's a far cry from the double agent concern that you had before: about an organization's actually being penetrated by someone malevolent.

Haave: There are still many countries out there that run very capable intelligence services. They are still collecting against the United States for a variety of reasons, both to determine our plans and intents and to gather our technology secrets. That has not changed.

Student: I'm sort of playing devil's advocate, but it occurs to me that if the technology itself is something that we're not necessarily going to maintain control of, then maybe the key to successful command and control is actually what you do with the information. I don't mean so much how well you process it but how you decide to proceed from that point forward. One of the readings asked how capable we would be if all our technology were destroyed or somehow

people weren't connected anymore.[4] How would we be able to operate? Is that just naïve? Is that really not an option?

Haave: What is so amazing about the U.S. military is that the soldiers, sailors, airmen and -women, and marines have such amazing adaptability that if systems go down (and clearly they do) the troops are able to resort to other means. We have a lot of technology that was built for a particular purpose, and they are very able to figure out other purposes for which that technology might be used. So there is a large degree of ingenuity, resourcefulness, adaptability, and flexibility that people have when they're in a crisis and they're put under the gun, so to speak, when something doesn't go as planned. The truth is that nothing ever goes as planned. There hasn't been an operation I've been involved with where something—usually communications—has not failed to go as planned. If you can count on anything, it's that communications will fail.

Student: We often hear nowadays that technology is moving so quickly that systems become obsolete a year or two after they come out. How do we ensure interoperability between systems while staying on the cutting edge of technology?

Haave: I don't think you drive interoperability among systems. You have to drive it at the data level, not at the system level. We have to get to a data level of interoperability, where data can be shared regardless of the platform, the operating system, the application, or whatever. That will allow us to have the interoperability we need. We have tried for years in the DOD to drive interoperability at a system or platform level and it hasn't worked. It's not going to work, and the definition of insanity is to continue doing the same thing over and over and expect a different result.

We have to get to data interoperability. DARPA conducted a program out at Pacific Air Forces to do exactly that. Whether it was a structured or unstructured database didn't matter. What the system would do was pull the information relevant to a particular problem using automated software agents and bring it into a space on a machine. It could be any one of your machines. It was tailored for your use, but it was all the same data. Everyone was using the same data, but using it for different purposes and tailored to the way they needed it. That's where we need to go in the future.

What happened on that particular project, which was really interesting, was that we found out where all the dirty databases were. There were databases that people didn't use, or there was only one bit of information out of that database that people used, but we're paying oodles of money to maintain those databases for no really good reason.

Student: We talk about terrorists all the time. Professor Graham Allison over at the Kennedy School has the saying that the best way to get a nuclear bomb into the United States is in a bale of marijuana, because it's so easy to get into the country. What are the DOD's concerns in this area? How do we protect not just against a terrorist threat, but against a terrorist threat using the organized crime, narco-trafficking, human trafficking chain to get things we don't want into our country? How is the DOD handling that aspect of this?

---

[4]Thomas Coakley, *Command and Control for War and Peace* (Washington, D.C.: National Defense University, 1992).

Haave: It is a huge problem for the Department of Homeland Security and it is a huge problem for the Department of Defense. You have to recognize that we have considerable borders that are not covered and we can't be everywhere all the time. The only way that I know to address the threat is to make better use of the information we have available to us and conduct the proper analysis. You might be able to know, through some means, that there is a nuclear weapon on board a ship, but how we know it and the extent to which we can know it may not be known. So I think you have to do it through analysis, and that's actually the point I want to get to.

We talk a lot about threat. There are a lot of threats to the United States. There are a lot of threats to the world, but the truth is that the likelihood of a threat may not be as high as we think it is. You have to look at the threat in context: in the context of vulnerabilities, likelihood, means, countermeasures, and the application of resources. So I don't think it's good enough just to think about the threat, because there aren't enough resources to accommodate that. We have to find a method by which we allocate those resources. To create a risk methodology is one way of doing that.

Will we be right all the time? Absolutely not. Do I think there will be other terrorist incidents in the United States? Yes. Information and intelligence are not a science: they are an art. We are not, despite what people say, Big Brother and all-knowing, all-seeing, omniscient, omnipotent, et cetera. I do think we have a lot of capability to do lots of things. Frankly, from where I sit, I can tell you for a fact that tremendous numbers of potential events are thwarted every day in this country. Unfortunately you don't get to hear about all those.

Student: I'm struck by how much technology we have and by how much information we can get, and I know that's part of your expertise, but I want to go back to the element of HUMINT. Many have argued that there needs to be a balance between HUMINT and technical information that is gathered. The problem I have with HUMINT is that people have different interests and are promoting different interests. We're in a country with so many ethnic and religious minorities that we have a conflict of so many different interests. Do you see that as a huge problem for the United States and for the intelligence community here?

Haave: I personally do not see it as a problem. In this room, we all have different interests. We all come from different cultural backgrounds and different economic situations. We have lots of experience, lots of expertise, and lots of knowledge. We live in a global world, and I think that the extent to which we can understand other cultures and other systems, if you will, only helps us in the world in which we live today. I don't find it a problem, because I like the perspectives. I think there is value in every bit of information that comes to our attention, and it makes us better. It also helps to underscore that we're all human beings. We're on the planet, we all have a right to be here, and there is a certain amount of respect due each and every individual. That's my personal opinion. I actually think it's a good thing.

We're having a huge philosophical debate about HUMINT right now in the department, because, as you know, we've decimated the HUMINT capability of the intelligence community over the past couple of decades and now we're trying to resurrect it. One of the issues in the discussions we're having is: What exactly is HUMINT, and what do you want it to do? Is it overt? Is it something clandestine? I think we have to get back to the basics of what it is and what

we want it to do, and then we can talk about how we are going do it and what the best means available are.

I don't think we've figured that out. I will tell you that it is different from the way we did HUMINT collection in the past, because it's about more than individuals now. It's about networks and leveraging networks—whether networks of systems or people—and I'm not sure we have come to grips with what that looks like.

Oettinger: Continuing on your point, and to add to what Carol was saying, my colleagues across the way at the law school are focusing on "Don't ask, don't tell" and women's issues in the military, but leaving that aside for the moment, the military is probably more advanced than any other segment of our society in making effective use of the wide diversity of the people in the United States. This is not necessarily as true of the civilian parts of the intelligence community, where, heaven help us, an Ivy League-ish kind of cliquishness, which is historically understandable, nonetheless remains. I would add to Carol's statement that there's need across the board for progress in reducing the degree of xenophobia that prevails in some parts of the intelligence community and therefore deprives us of one of our best assets. I take the personal view that it is enormous foolishness to fail to make total use of one of our greatest assts, which is that we're one of the few countries in the world, if not the only one, where people with all sorts of different backgrounds can really live harmoniously and give vent to disagreements by voice rather than by Kalashnikov.

Student: I want to ask about inefficiencies in information security and counterintelligence, and I'll try to make an analogy. My understanding of the reason the long-term capital hedge funds fell is that they got so wrapped up in trying to root out inefficiencies that they leveraged themselves too highly and didn't manage the risk properly. If you think about the leaking of classified information and the draining of U.S. technology as an inefficiency—a drag on the system—and you also think about protective measures as inefficiencies and drags on the system, is there a balance where we can tolerate certain inefficiencies and don't wrap our hands so far around the problem that we lose sight of other things and end up spending too much money?

Haave: In my vision that's where we are driving to, because even though we have not applied all the resources against it that we might, our strategy in the past has been to be risk avoidant or risk averse. We can't afford that. We can't get there from here. We have to make some decisions about how much risk we're willing to take under what conditions.

Driving the DOD to a risk strategy is very difficult, because for so long we've lived in the environment characterized by the story about Khobar Towers and what we've done in terms of decimating the leadership. As a result it's very hard for people to become comfortable assuming risk for fear that something is going to happen to their careers.

You can see it in a variety of ways. One of the things in *Black Hawk Down*[5] (and I know several people who were in Mogadishu) is that they rappelled out of the helicopters, of course the big ropes come down, and people actually risked their lives to get the ropes. That's because there's a cost to those ropes. The troops are trained that way. You don't leave things on the

[5]Mark Bowden, *Black Hawk Down* (New York: Atlantic Monthly Press, 1999).

battlefield. Everything costs money. So how that translates in people's minds is very interesting, and not particularly efficient in some cases. Of course, there's a difference between what we do in peacetime and what we do in war. You would think people would take more risk in war, but the fact that we spend much of our time in a peacetime bureaucracy does not necessarily translate into what we do in wartime.

Student: Soldiers revert to training. I'm a colonel in the Army, with a background in Special Forces and intelligence, and we had a similar experience. In peacetime parachuting, you can't just leave your parachute in the drop zone. It's an expensive piece of gear. You've got to roll it up and carry it off into the truck. Guys were jumping into Grenada and Panama under direct fire and rolling up their parachutes, and the NCOs [noncommissioned officers] were saying, "No, this is combat. You don't have to do that."

Haave: But that's the training. Military training is fabulous. I was one of the first women officers actually to go to airborne school and learned how to fall and do all those things. Much more recently, I was rollerblading down the road and we'd had a storm, so there was sand across the road. As I came down a hill on a curve, I hit the sand, my wheels locked, and I flew forward. I did a perfect parachute landing fall (PLF) and you can see it to this day, because I still have marks where the sand rubbed into me in various places. So you revert to what you know. I can still do a PLF today. The military training is very good. It's rote. They drill it into you over and over again, and you absolutely will remember it when the time comes that you need it. So they will revert to what they're trained for.

Student: You talked about incentive problems in intelligence and you talked about risk management in the military. Does the DOD have a bunch of economists on its payroll who are trying to figure this out or is it all learned from what the last people did?

Haave: I don't know how many economists we have on the payroll. I would venture to say not many. I have hired some on contract to help me look at the risk methodology we want to use and start applying it in the department.. I like economists and anthropologists and behavioralists and all those kinds of folks, because I think those are areas to which we have not devoted enough attention. We seem to be very comfortable doing things the same old way, and I think there are other perspectives and other energies to be brought to the table. I actually have a lot of experimentation going on with open source right now, having to do with economists and anthropologists and those kinds of folks in different areas.

Student: You talk a lot about risk management. Suppose you come up with a great formula that you think is going to work really well. How do you then communicate to military and civilian personnel that they're going to be told: "You're really not a high priority anymore. We're not going to give you everything you want." How do you deal with this internal, organizational, public relations nightmare?

Haave: There's a baseline level of protection that everybody needs to be afforded, and then there are some assets that probably have higher priority than others. Those tradeoffs are made every day, whether in business or in government, and in the end you have to make those hard choices. I'm not talking about reducing the level of protection to a point where we don't have fences

around military bases and those kinds of things. But, for example, there are some things in the critical infrastructure arena where you have single-point failures, and the question becomes "Can you afford to have that failure in that particular instance or with that particular asset?" Those are decisions that have to be made every day using cost-benefit analysis and several different tools at our disposal.

In my department I have people—and, bless their hearts, they're great people—who have been in the Pentagon for thirty years and have not left it, so when they write policy, they write it for the Pentagon. That doesn't really work for somebody who's in Iraq, because the situation and the conditions are different. When I took this job I said, "We're going to write policy differently." Something that we had not been good about doing, which I've now implemented, is that we are now costing the policy, because some policies that we write are just not affordable. If you're not actually going to implement it because it's not affordable, then why write it? That way you get into managing by exception and waiver, which is its own conundrum. It's a very difficult problem, but when my folks write a policy I ask them to do a cost/benefit analysis for the department.

We're also doing an experiment with blogs—Web logs. The reason is that when we write policy, we send it out and get everybody's opinion and chop on it. The Joint Staff usually represents the various geographic and specified commands and sometimes what they report back to me is not exactly what the commands might have told me had they been given the opportunity. What I'm now doing is starting to put draft policy out in the form of blogs so that people can chat about it and give their feedback. I am actually going to disseminate policy via blogs rather than the hierarchical way it goes out today as an experiment. When we sign out policy today, the deputy secretary of defense signs it; it then goes to the service secretaries, down to the components, down, down, down, and finally, three years later, it may get to the guy who actually has to use it for some reason. In this day and age of electronic environment, we're experimenting with ways to get policy developed and distributed much more rapidly than we have in the past.

Oettinger: I'd like to add to what you just said, because it leaves the impression that policy is made deliberately, and by a rational process. I will give you an illustration of a more informal process in one realm that I happen to be familiar with, telecommunications infrastructure, where at least from the military standpoint the policy came about by happenstance and entirely externally.

If you look at the world through about 1984, there was a monopoly in telecommunications, where the protection, provision, and single-point-of-failure issues were addressed primarily by one civilian supplier. The whole regime is too complicated to discuss here, but basically anytime the Pentagon wanted something done it got done pretty well and it got plastered onto everybody's phone bill in a manner that nobody noticed, because it might have made a difference of 1/100th of a penny on each person's bill. The policy essentially was made as economic policy in the Federal Communications Commission, not as rational policy in the Pentagon.

To this day, for a variety of reasons, the military still relies extensively on commercial telecommunications. So what happened after 1984? During the transition, the Defense Department argued vehemently that it was going to go to hell in a handbasket if the old regime didn't remain. Fast-forwarding through many agonies and reorganizations that are still ongoing if

you look at the headlines of the last couple of days, under the new regime you essentially get a lot of investment—for example, in dark fiber—that the Pentagon would never have made rationally, but exuberant entrepreneurs put their money into the ground. So there's a certain amount of redundancy. It's totally unplanned, and it's causing a number of people to go bankrupt, but there it is as fiber optic capacity. I don't vouch for the accuracy of every detail in this quick summary of a twenty-year history, but I just want to put it on the table as an illustration that policy sometimes just happens, and the world we live in is a mixture of what Carol has described and things that happen on the way to the Forum but were unplanned.

Haave: I'll give you another example. We were working on a wireless policy for the DOD. My counterpart, who is the deputy chief information officer for the department, and I had been involved in this whole process. The draft policy showed up on our desks, and she and I, independently in our offices, read it. It basically banned all wireless technology in the DOD, to include combat radios. I got my guys in, threw my hands up, and asked, "What is this? We're not going *less* wireless; we're going *more* wireless! We need to figure out a policy that is going to accommodate that reality. We won't restrict the use of wireless technology. We can't stop the progress of technology. We have to be able to get out in front of the technology, have some concept of what it's going to do within the organization and to our operations, and then try to write policy that is at least coincident with it." Right now the policy is so far behind the technology that the technology is out of the barn, over the hill, and through the dam or whatever before we even get our eyes on it. So one of the things I've done is hire people whose sole purpose is to look at technology in the future and try to get us ahead of the policy game. It takes a long time to write policy.

Student: I agree that we have no choice when formulating our security strategy but to go to some sort of risk management-based approach. I read the recent journal articles and news magazines about "The likelihood that you will die in your car is much greater than the likelihood that a little terrorist group will smuggle in a radiological device." I agree, but the problem is that risk is generally actuarial, based on past statistics and behaviors. Yet we're facing kind of a protean enemy: a new war on shadowy fronts. With this enemy you have elements of disastrous impact (even though the chances are small), frangibility, malleability, and change that are not actuarial and that you just can't program. That tells me that risk management sounds good, but in war it sometimes goes out the window.

Haave: I don't disagree with that. I think in the end what we have to focus on is being much more proactive, much more aggressive, and much more predictive in our analytic capabilities. We are very good at analyzing the past, fighting the last war, and all those things. It is a culture change for us to look at predictive analysis. Several programs have started that are in fact looking at just that: taking the lessons learned from the past and also looking from a predictive standpoint. You can do it mathematically, you can do it socially. There are a number of ways to approach the problem, and there are a number of initiatives underway to look at that.

Student: We've been talking about risk management, and about being more predictive about the future. I know you've had some experience on Capitol Hill. How do you get the public to go along with risk assessment? You've said we won't always be right and we won't always be positive. For example, how could you have gotten the public to go into Afghanistan and get

Osama bin Laden before 9/11? How could you get people to wait in long security lines at the airports and pay for installing cockpit doors before there were possible takeovers of airplanes? It seems that predicting the future is very difficult for the intelligence community, but it's even more difficult to have the public go along with it and authorize the intelligence community to take steps, particularly when we all know there's ambiguity in their predictions.

Haave: You have to make the best case that you can make. There is an awful lot of information out there, a lot of which we don't and can't process, some of which we use, some of which we don't. I think you have to come up with what I call structured arguments. On the basis of your analysis of information you can create theories about the future, model and simulate those theories, attach probabilities to them, and make some decisions about them. That's probably the best we can do.

There is also an art; we call it operational art. It's the way we fight wars, and the more experience you have in the department and in the military the more operational art, or expertise, you have. So I think there are several things we can do, but in the end it's a tradeoff, and at some point you have to decide you have enough information to make a decision and move forward.

With respect to the U.S. public, we are in an interesting time. This is my personal opinion (and I know this is being recorded so I have to be very careful). The media have a lot of influence over what the American public decides about something. To the extent that we can make a logical, rational case to the media, and they are willing to publicize that case, it helps us. But, frankly, I don't think we've progressed much since the days of Roman gladiators, when people got into the ring and were mauled, stabbed, javelined, or whatever-ed to death and people sat in the stands and cheered.

I can give you a real story on this. How many of you know the Nantahala River in North Carolina? The highest class rapids in the river are level III. The bottom line is that at the end of the river there is a huge hydraulic place where the water turns over on itself and churns, and if you get caught in it you get stuck. So what happens at the bottom of the Nantahala River is that you have these two-person "funyaks," these little collapsible kayaks, and then you have six-person rafts. Two people come down in a two-person funyak, hit the hydraulic, and they both are thrown out of the boat. The woman goes down the chute and the man is stuck in the hydraulic. He comes up. He churns down. He comes up. He churns down. People are trying to throw him ropes. In the meantime, you have to picture that there are people on the bank sitting in lawn chairs and drinking beers. As he comes up, and he goes under, and he comes up, and he goes under, they are clapping and cheering. They think it's great fun.

We have a society that loves to see people either get destroyed or self-destruct. We're very narcissistic that way. I know this is off point, and it was a free association on my part, but I do think there is an aspect to the media that we may not have figured out how to harness yet.

Student: In light of the difficulty of finding weapons of mass destruction (WMD) in Iraq, if you go back to before we attacked Iraq and do all kinds of different analyses from a game theory perspective it would seem very probable that there were WMD there. With the backlash from this, it seems to me that policy makers of the future are going to be even more reluctant to perform risk assessment and act on that, although with Iraq it would have been a rational thing to do. Do we as

a society need to be more accepting of risk assessment that uses the best data that we have, and be willing to accept that sometimes we get something wrong? Do you think that it's possible for our society to take on that mindset, and do you think that is good or bad? How do we avoid becoming even more risk averse in the wake of what happened?

Haave: We have an arrogance about ourselves that would imply that we are always right, and the truth is that we are sometimes wrong.

Regarding WMD in Iraq, one shouldn't forget that Saddam Hussein did gas his own people. There were a number of indicators that would have led you to believe that there were WMD in Iraq. I believe, not on the basis of anything in particular, that at some point we will find them. You should also not forget that there were MiGs buried in the sand. Nobody would have figured that those MiGs were buried the way they were. As we go through buildings, and knock out walls, we find millions of dollars stashed in places you wouldn't expect money to be stashed, so clearly the regime was very creative in the way it hid things.

It is a real danger that we will become risk averse, because we are very reactive and the public is influenced by a lot of what they read in the media and see on television and hear on the radio. I think it is an unfortunate situation that we will find ourselves in if we are not conscious that intelligence is an art. We may not have all the information, but at some point we have to make a decision. If we wait for all the information we'll never make a decision, which is its own decision in some respects.

Student: On the subject of risk in Iraq, given that Saddam Hussein had gassed some of his people and had gassed Iranians, I would think the non-risky action would be to intervene. The risk is that if we don't, how much longer can we wait until the weapons are used against us?

Haave: We have no way of knowing that. That is what makes this so hard. To the extent that we have some indications and warning, they can feed the theory, or the postulate, if you will. Since he's not there anymore, and there's been an intervention, we don't know how to answer that question. We don't know what we don't know.

Student: Let me offer a personal anecdote on that. I'm a civil engineer in the Army, in the Corps of Engineers. I was in Iraq last spring. My company at the time was going to build a refueling point halfway between Baghdad and Kuwait City. In a 100-acre space (and keep in mind that Iraq is the size of California) where we were clearing and grubbing and stripping the land off so that it was flat and we could put in these big fuel bladders, we ran into two bunkers of stuff buried in the middle of the desert. They were not near anything. This is desert where you can stand and look in all directions and see nothing but sand. It was very tense for my bulldozer operators every time they hit one of those, because we didn't know if we were hitting a biological or chemical weapons store. It wasn't very comfortable at 130 degrees in a chemical suit, but we survived. So there is a huge statistical possibility that there will be WMD found in Iraq. It is a matter of time and I think it is a "when," not an "if." It may be after this election, it may be in ten years, but they will be found.

Student: Speaking of laughing at people in great danger, Bush the other day made the comment on a news show that he's a war president and there was a lot of laughter here, at least in Boston,

in the letters to the editor and so on. I know that your boss's boss believes that we are at war. I really do think that one of the problems about risk assessment, reaction to risk, and everything else is that some of us believe that we are at war and this whole set of scenes needs to change. The majority of us really don't get it yet. The way we did force protection when I was in the Middle East was predicated on our being in a long war, so we said, "Hey, give the sailors a break, they've got to get off the ship." Even though it was risky there was no risk avoidance there. It was: "Take a break, because this is a long war." But when you get back to the United States there isn't that same feeling that permeates down below, or even outside the Pentagon or Washington, D.C. If you really believe that you're at war, it has a lot to do with how you organize your intelligence resources: how you react to risk, how you allocate, and the amount of risk you take.

Haave: That's right. We have one way of behaving in peacetime, and another way of behaving in war. We traditionally go to war with a peacetime bureaucracy.

I'll give you an example of that. I was part of a management team that ran a program for Secretary Perry in 1996 called the Bosnia Command and Control Augmentation Initiative. It was designed to improve the communications and information infrastructure throughout Europe and Bosnia using coalition-friendly commercial satellite communications technology. Fast-forward now to Kosovo. We now had Predator, and we wanted to do precision targeting with Predator. For the want of one VSAT [very small aperture terminal] we could not make the system work. I knew that EUCOM [European Command] headquarters had a VSAT receiver, so we called EUCOM and got a lieutenant colonel on the phone. He said, "But we don't have a requirement for that." They wouldn't give us the VSAT receiver. Now, understand that this Predator was sent over by the chief of staff at the time on two dedicated C-17s: not an insignificant chunk of change to get this capability over there. So I then had the two-star write a requirement, which he signed out and we then forwarded through the chain, so we could get the VSAT receiver.

What's the point of that? The point is that in this bureaucracy we are not only asking people who are at risk to conduct their operations and work their eighteen hours a day and do all the things they do; we are also asking them to do the paperwork to get the bureaucracy to support them. To my mind, there's something wrong with that. You can't have these guys do it all. Somebody has to be in support. Now, it's interesting, because the tooth-to-tail ratio, depending on the organization, is very high. There is a lot of support to shooters, however you want to define "shooters," and yet they still have to do all the paperwork to push the bureaucracy to do its job. It's just amazing to me.

Student: I've heard from one person that the risk is not attacking, and from someone else that the risk is attacking, and that there's a probability of one that there's stuff in Iraq. You hear a lot of numbers thrown around, but no one has a methodology for getting these numbers. You have methods for defining risk. Who in the DOD figures out what methodology is going to be used to come up with *P*, where *P* is the probability that there are WMD somewhere in Iraq, or that if we attack Iraq a certain percentage of the weapons will go over the border and hit some group we don't want to have hit? Where do these numbers come from?

Haave: They come from several different places. One is the collection that we do, whether it's HUMINT or technical. Another is the analysis we conduct, the art of strategic information, if you

will. There are people—policy makers and decision makers—who have different viewpoints, knowledge, background, and experience. You can assign those factors a number.

We ran a program at one point that was based on influence. It tried to assign probabilistic numbers to various things. Basically, you have a person of interest, and that person can be related to, or influenced by, some other person. Depending on the degree of that relationship, we assigned it a value, and then did an experiment based on that value. At the time I was working for DARPA, and I wanted to model the DARPA leadership. We thought it would be fun to do that with the director at the time (although we actually didn't do it). There are people and organizations in the community that do these kinds of things. DARPA is one of them. I have an ongoing program looking at some of that, but if you're asking me if that's the way they make the decisions systematically, I'm not sure it is. I think it is a factor in a decision, but not necessarily the only factor.

Student: Going back to several topics ago, we often talk about technology. The word means a lot and we rarely break it down into its components. In your opinion, what aspect or piece of technology has advanced intelligence and counterintelligence, both gathering and analysis, and what has been a detriment to that process?

Haave: I'll give you two sides of the same coin. Data mining can be used for good or, as some might claim, for evil. However, it does provide us with information we didn't have before. For example, when I was involved with organized crime investigations back in the late 1970s and early 1980s it was a manual process. You had a mob boss who was connected to numbers of people through personal relationships and through companies and businesses. We did that link analysis in our heads. When we went to trial, it was a very lengthy, stressful process to build those cases manually. Computers have infinite capability to make those links faster and better than we can. So that's the good side. If you want to go after a terrorist organization and look at its money (and I would argue that if you want to break the backs of the terrorist organizations you should follow the money, which is not unlike what we did with organized crime), computers can do that much more easily than the manual leads we used to chase.

There is much more information available to us now than there was before. However, as we found out with the TIA program,[6] there are also privacy implications that people are concerned about. I will tell you that TIA was not collecting information on U.S. persons. The TIA program—DARPA—was providing the tools by which intelligence analysts could mine data, perform link analysis, and come to conclusions about foreign intelligence activities.

Oettinger: It should be added that John Poindexter is a sweet man, and a very bright one, but putting him in that position was a priori sort of excessively naïve and the public relations consequences were terrible.[7] The road to hell can be paved with all sorts of things.

---

[6]The TIA program, run by DARPA's Information Awareness Office, began in 2002 as the Total Information Awareness program. The name was changed to Terrorist Information Awareness program in 2003. For background on TIA, see http://www.isn.ethz.ch/researchpub/publihouse/infosecurity/volume_10/C3/C3_index.htm (Accessed on 10 May 2004.)

[7]Admiral John Poindexter (USN, Ret.) headed DARPA's Information Awareness Office while the original TIA

Haave: And DARPA didn't help itself by some of the statements they made.

Student: Can computers mine this influence space for discrete transactions somewhere along the line in this asymmetric mode?

Oettinger: Computers can do things faster than people, but the output is only as good as the data. That gets us back to a combination of technical and human intelligence, which is where the real problems and the real investments are aligned. Garbage in, garbage out remains a consideration, no matter how good the computer processing.

Haave: There has to be a balance between the technical intelligence and the HUMINT. How much of which is enough? That's an ongoing process that we debate every time we come to a budget cycle. How much technical intelligence is enough, and how much HUMINT is enough?

Student: A week ago I saw Arthur Cebrowski's latest transformation briefing.[8] He had a graphic that plotted the amount of information against the number of analysts, and showed the huge delta. I guess his solution was that we all—all decision makers and all policy makers—would have to become our own analysts, because there is too much data. Many decision makers in your position were analysts at some point in their careers. I'd be interested in your thoughts abut the differences between decision-making and analysis. Do you now get analysis presented to you or do you want to do it yourself? What do you think about the Cebrowski curve?

Haave: I think the Cebrowski curve is right. There is a huge gap.

It's interesting. Back when I was a contractor two-and-a-half years ago, I used to tell my general officer/flag officer friends that the more stars you have the less useful and real information you get. That is because at each level, as information goes forward to the leadership, it is churned and mitigated and people make decisions along the way that "The boss doesn't really want to do this," or "The boss wants to do that." I personally prefer to have people come forward with the information and with options: pros and cons. The truth is that I'm an investigator and an analyst by trade and I have a tendency to want to do my own analysis.

What you find with most general officers, flag officers, and leaders in my position is that you come to trust some number of people. If they come to you and they say, "Boss, this is the right answer," you have a tendency to trust them and think "I believe you." There are other people whose staff work may not be as thorough, and when they come to you and make that same claim you might hesitate a bit and think about it-- and do your own analysis.

So it depends on the situation and where you are in the process, but you can't wait for 100 percent of the information. You just can't get there. At some point that operational art, that instinct, has to come into play, and that's why you can't just rely on probabilities. There are instincts. There is operational art. There are ways of maximizing and taking advantage of your experience and education and things you've done in your life or places where you've been, and

---

program was in place.

[8]Vice Admiral Arthur K. Cebrowski (USN, Ret.) is director of military transformation in the Office of the Secretary of Defense (OSD).

you can't discount them. In some cases, they are probably more important. I am not the smartest person in the world (in fact, I'm probably not as smart as most of you in this room) but I have absolutely good instincts. I know what is right in most situations that I deal with, and I'll make a decision without all the information.

The truth is that if you don't you'll just churn. You have these IPTs [integrated process teams] with fifty people in a room, and nobody can agree. They'll continue on and on having a debate and trying to influence one another, and not necessarily move forward. At some point, that has to get kicked up to the leadership so that someone can make a decision. In the end I will always make a decision, even in a void, because at least we can move on. If change is constant, you can't afford to stay stagnant, and any decision can be changed. If you can convince me I'm wrong I'll change it, and I do it all the time if convinced.

Student: In the context of change, I wonder if you could talk a little about the relationship between the secretary of defense and the Joint Chiefs of Staff [JCS]. There are all these stories about real acrimony between them and the military's being unwilling to transform, et cetera.

Haave: I don't see that acrimony, actually. I work for the secretary of defense on the OSD side, and then you have the chairman and the JCS on the other side. The truth is that, in large measure, we normally see things the same way. The debates I have been in on various topics usually aren't at major levels of confrontation. Clearly, people have opinions as to what capabilities are required for what, when, where, why, and how. There is a debate about what the threat is and what the likelihood of that threat is. There is a debate about whether we should organize more for transnational, terrorist kinds of threats, maintain the peer competitor kind of posture, or prepare for a combination of both. That's not necessarily acrimony. Those are legitimate debates being conducted at the highest levels so that people can make the best decisions. I personally find them refreshing. Frankly, I think it would be more problematic if we weren't doing that.

At the end of the day, the secretary of defense is in fact the secretary of all defense, and has the ability to make the decisions that need to be made. But, as you know, there is a political process, and all sorts of things that come into play when we make those budget decisions.

Oettinger: In a somewhat related vein, your title has an element of counterintelligence in it. Your office was created fairly recently, somewhat simultaneously with the creation of the national-level counterintelligence executive.[9] Can you comment a bit on what that reflects, either coherently or incoherently?

Haave: The national counterintelligence executive was created basically to create a national strategy for counterintelligence and protection within the U.S. government, specifically as it relates to the CIA, FBI, and other agencies in the DOD, and to look at how we're spending our money across services and agencies. Are we doing the best we can for the taxpayer?

Counterintelligence was always a part of the DOD. In my previous job, counterintelligence was in my job jar, if you will. It is clearly something that we continue to be concerned about.

---

[9]The national counterintelligence executive was established by Presidential Decision Directive 75 on 5 January 2001. See URL: http://www.fas.org/irp/offdocs/pdd/pdd-75.htm (Accessed on 27 February 2004.)

While I agree that nation-states may not be the looming threat of the day, they are still running intelligence operations, and so are terrorists, organized crime, and lots of other folks, so counterintelligence is still important.

If you go back to the National Security Act and Executive Order 12333, there is foreign intelligence and there is counterintelligence. They are two sides of the same coin. The information that we analyze on both sides is the same; it's just that the perspective is different. I am interested in knowing what the adversaries know about us, how they know it, and what we're going to do about it, whereas on the foreign intelligence side they're interested in knowing about the adversaries' plans and intentions and those kinds of things. We use the same data, but we analyze it from a different perspective and the actions that we take as a result are different.

Student: There are good things about everybody working together and getting their different perspectives together. At the same time, people end up looking at the information through the specific lens of their training. What if we started training people in intermediary programs, where you are never just a CIA person but actually your specific training is to be a link between two organizations? Is that impractical?

Haave: When you say "a link between two organizations," describe what you mean. Are you talking about a liaison?

Student: Yes, a filter that doesn't come from one organization or another.

Haave: We're sort of doing that at the TTIC—the Terrorist Threat Integration Center—where you have all the agencies coming together and bringing their information and authorities. That organization is brokering, if you will, information that is distributed to other places. It's part of the way we will get to information sharing. Right now, it's more a manual process. In the future you want it to be an electronic, automated process. Will we get there? Yes. Is the technology there? Yes. Culturally we have to change, and we have to be willing to do that.

I will also say that you need those brokers today, those middlepeople to facilitate the sharing (I call these hostage exchanges), because the truth is that CIA's information is not CIA's information, and NSA's [National Security Agency's] information is not NSA's information. It is the U.S. government's information, so policymakers must decide what, when, where, why, and how that information gets distributed, and for what purposes, by whom, and to whom. We must move from being collector driven to consumer driven.

Oettinger: That's true in principle, but in practice people who work in intermediary positions do not necessarily get rewarded by their own institutions. There are very few intermediary organizations with a hierarchy or reward structure. This goes back to the conundrum that Carol posed earlier about how you construct a reward structure that will encourage and reward people who do what you describe.

Haave: Actually, you have to have twenty-seven lives. I've probably used up twenty-five of mine, because you do get killed in this process if you're a change agent. The bureaucracy doesn't like it. You have to be able to pick yourself up, dust yourself off, and at some point regain the

energy to go back and continue doing what you're doing. It is very trying. It is very disheartening at times.

But I think there are ways to do it, and I'll give you examples. Secretary Perry's program, which I mentioned earlier, was called the Bosnia Command and Control Program. It was his personal program. The reason it was so successful is that it was a $100 million program that went operational in three months. That's unheard of in the DOD. I doubt that we will ever, in my lifetime, have another program that equals it.

Why was it successful? Because it was his program, and we had his top cover. It was implied, we never used it, but it was clear to everybody. The assistant secretary of defense for command, control, communications, and intelligence at the time[10] wrote an email to his friends, and I have a copy of it. It began with about seven lines of "Close Hold." It said, "To those of you who are my friends: Either get on board or get out of the way. You will not survive being an obstructionist." That is a very powerful statement. It was clear to people that there were going to be repercussions if they didn't do what we were trying to do, which was operationalize a direct-broadcast VSAT capability to thirty-three sites in Europe and Bosnia. You need that level of interest, that top cover, that passion, if you will, at the top, if you want to make it work.

It's very easy to get diluted by what it is you do every day, because there is so much to do and there is not enough time to do it. But where you have focus, where you have authority, where you have power, where you have budget, when all of that confluence occurs, it works. The key when you're trying to make change in organizational structures is to make sure that you have the right leadership in place, the right authorities, and the right presence of power.

I was telling the lunch group earlier that I spent a year in Purgatory at what was then the National Imagery and Mapping Agency; it's now the National Geospatial-Intelligence Agency. We were taking seven disparate organizations, putting them together, and thinking that they would play nicely. But the truth is that when you're trying to make a transformation or fundamental change in an organization 20 percent of the total population will be for it. They like change; they are comfortable with change, et cetera. Fifty percent will sit on the fence and see which way the wind blows, and 30 percent will actively oppose you. If you do not have the leadership in the 20 percent, I offer that you will not make the transformation you hope to achieve. You just won't get there.

It does make a difference who is in what position. If you look at the government, it makes a difference who the director of central intelligence is. It makes a difference who the secretary of defense is. It makes a difference who the under secretary for acquisition, technology, and logistics is. To the extent that they are friends, share common goals, and have a propensity to want to get things done instead of studying it (which I vote for) we will make progress. To the extent that you don't have these things, we will remain in the status quo.

You see in the Army, for example, that General [Peter] Schoonmaker was brought in as the Chief of Staff by the Secretary of Defense to make changes in the Army. One should assume that there is a close relationship there. So people can and do make a difference.

---

[10]Emmett Paige, Jr.

Oettinger: If you want another instance of that, there is a presentation in the seminar proceedings by Charles Stiles about the installation of the technology in the Sinai Desert separating the Egyptians and the Israelis, which was put in during the Nixon administration.[11] Henry Kissinger played the role of providing cover, and Stiles's account of how the bureaucracy got hold of it and how everything was put into place is totally parallel to what you heard from Carol. It can be done, but it does require people to put their effort and their passion where their mouth is.

Haave: Good word! I love that word "passion," because the key for all of you is to identify your passion. If you want to make a difference in the world, in your environment, or in your space, you have to identify your passion and follow it. The truth is that it's not about money. We all have enough to survive. It's whether or not you're going to spend your life being happy and productive in what you like to do. I know a lot of people who hate their jobs. Some of them have actually worked for me. My comment to them is, "Look, if you're unhappy, we will identify what you are passionate about and what your skills and talents are, and we will find you another job." It does me no good, it does them no good, and it does the department no good to have somebody in a position in which she or he is unhappy.

Most of you are young. You are in a position to give serious thought to that, because that is how you will be most successful. Find what you are passionate about, whatever that is. That's what makes the world go around. We are all different. We all have different strengths and talents. We all have different motivations. I encourage and challenge you to figure out what your passion is and go forward in that direction, as opposed to something that is not as exciting for you. So much for my political speech!

Student: I had a question about the TTIC. It takes care of one problem (or attempts to), which is coordination. But it seems that a lot of civilian intelligence agencies have been more reactive than predictive in terms of terrorism, or at least that's what we see publicly. After the 1970s terrorism that went on, okay, now we're going to screen luggage. Oklahoma City happens; now we're going to put in surveillance cameras and have people looking for suspicious activities. Then somebody has a shoe bomb, so everyone take off their shoes.

Haave: Not to forget the plastic knives (as if stainless steel forks can't hurt us): my personal favorite!

Student: We're reacting to what terrorists have done in the past, and terrorists always find the next thing. They figure it out. So is there a lesson learned, or is there information sharing from the military to some of these civilian agencies that should be doing that? For example, in the Army, the Navy, and the other services you have these Red Teams where you actually try to predict on the basis of enemy doctrine, get inside their heads, and then have some separate Blue Team or operations group react to that and go back and forth. That may be something we should be doing with terrorism, even though it's really hard. To me, it's not necessarily communicating that

---

[11]Charles L. Stiles, "The U.S. Sinai Support Mission," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1991* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-93-1, February 1993), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=352

somebody is trying to take flying lessons, it's trying to look for somebody who is trying to learn to take off and fly but not land. That's suspicious, and maybe we should have been anticipating that terrorists might use an airplane as a weapon of mass destruction. I don't know if there's any thought given to that, or if there's an independent group that may do that type of analysis and is rewarded for it.

Haave: I think there is a movement toward doing more of those kinds of things. I am certainly a big proponent of that. You learn a lot by doing force-on-force and other kinds of exercises, with modeling and simulation, to determine where we are most at risk.

Oettinger: The future is inherently unpredictable, so the whole question of gaming, scenario building, et cetera, and what one can expect from it seems to me (and I don't know if Carol would agree or not) at best to sensitize you to see more out of the corner of your eye, because you get used to looking at alternatives. The notion that somehow, except by accident or luck, you can hit precisely what the other guy is going to do is delusion.

Student: CIA has a Red Team, and they put out an out-of-the-box product that is interesting for the intelligence community. But when you take that and want to go to a decision maker or a commander, whose field of view has to be uncluttered so he or she can decide, out-of-the-box thinking offers too many out-of-the-box possibilities for that decision maker actually to consider and act on. Therefore it really becomes just an inside, amusing kind of thing rather than something a decision maker can use.

Haave: But I will tell you that the extent to which we have identified and leveraged experts well in advance of a crisis will mitigate some of that surprise. For example, we in the Defense Department would not engage the community until we put out a Warning Order. Where you see us heading now is to know something about everything … all the time. What that's really trying to say is that we need to be better at predicting and anticipating trends that may come forward into our thought process and view in the future. So you see more in terms of advanced force operations, or predictive analysis, or understanding cultures and nations and terrorist groups much more completely than we might have in the past, and using different kinds of experts to help us do that. We are moving in that direction. That's what's going to be the key. Are we going to be able to predict all the time? No.

Student: I don't mean predict as in you're going to predict an exact incident, but what it might do is help, say, the secretary of homeland security identify where gaps exist in terms of coordination and how different agencies are going to act together. They may not only be government agencies. It provides you with a gap analysis to figure that out. I don't think you're going to know they're going to fly into the Twin Towers right now, but it may help you to figure out what happens if they do fly into the towers, and who is going to handle what. I was amazed by how well everybody reacted to that. There was a lot of just figuring out on the ground when people were not sure which agency would even be in charge.

Haave: The military actually, as you know, does a lot of exercises. Those exercises are geared toward exactly that. What are the relationships? What are the command and control relationships, the reporting relationships? What is the role of the military with regard to homeland security?

What is the homeland defense mission? There have been a number of exercises that are designed to address all those kinds of questions: both tabletop and modeling and simulation and other, more real-life kinds of simulations in the real world.

Student: Whenever I hear this it scares me. I've never been in the military and probably never will be, but I've spent all my time in the laboratory doing experiments. You get really good at predicting the mean. We can tell you how the mean is going to move. After a point, just knowing the mean is not all that interesting.

I'm very impressed by the military. When we went into Iraq, I said, "My God, we really are amazing at fighting this war! We can do things that I don't think anybody in the civilian population realized we could do." But when people start saying, "We should have predicted something like September 11," I say that you're really looking at outliers here. Our statistics, our probabilities, can't predict the individual outliers. They will actually surprise you. I'm wondering how you convince the public that the outliers can still get you?

Haave: When you look at the huge amounts of information that are out there in the world, orders of magnitude beyond what we can even imagine, it is hard to believe that we would be able to predict accurately something as well in advance as we might. One of the interesting things about Khobar Towers, the bombing of the barracks in Lebanon, and the *U.S.S. Cole* is that we come at those things in hindsight. So you have a postulated theory, which is the event, and then it's very easy to cull through information to support your theory. It is much more difficult to do that in advance of an event. So, while there are lessons learned and clearly we need to learn them—and I think we are learning them—I don't find necessarily that going back and looking for the smoking gun, if you will, is particularly useful. I think it would be more useful to look for the smoking gun in advance of the actual event. But we are spending an enormous amount of time in the department, the CIA, and the FBI answering questions on "What did we know, when did we know it, and what did we do about it?"

Oettinger: There are some serious and important tradeoffs, and I'd be interested in hearing your view on them. If you go at it prospectively, then you need to know what's normal so that you have a background against which to see the figure of the abnormal. The normal can encompass damned near everything in sight. That means that you need to know about things that may never have anything to do with any incident. For instance, if you want to find the smoking gun before it smokes you may need to scan every gun transaction, and the political consequences of that are clear to everybody in this room. What kind of tradeoff would be made, and at what point? After all, it's not just a matter of buying the gun in the United States; you could buy it in Canada or Mexico and bring it in hidden in a bale of marijuana. So we're talking about global gun registration and control for somebody—never mind the question yet of who—to be able to detect through link analysis that this gun purchase leads to something.

Haave: Here's an example. For some weapons, you have to get a special weapons license. You can be cleared to the highest levels of security and it can still take a year or more to fill out the forms from the Bureau of Alcohol, Tobacco, and Firearms. Do you think that a terrorist is going to do that? No. So people who are law abiding will be in the database but the bad guys most likely will not be.

Oettinger: You've got to have informants all over the place to tell me that Joe sold a gun to Bill.

Haave: We do. There are a number of informants who do come forward and say, "You know, there's something not right about my neighbor." And there may or may not be something that is not quite right about that neighbor. The problem is: How many resources do you have to apply to these types of situations? How do we prioritize the activities?

Student: By no means would I be confident of implementing plans to stop or even think about attempting to stop this by going through all the gun licenses. You could get bogged down in detail and we already hit the problem that we have so much information that we can't manage it. While it's a possibility, it might not even be a viable plan of action.

I think you can discuss the issue in more general terms, although I don't know if this would get you any mileage. You could think about trying to get into the mind of people who think like this, and what they're after. Hitting the Pentagon means hitting the control center of the military operations of the United States. What else are they interested in? I know some work has been done, but could you concentrate efforts more on that instead of going through the details for individuals and getting bogged down in too much information?

Haave: Clearly we're doing a lot of that. We have behavioralists, psychologists, psychiatrists, anthropologists, historians, economists, religious experts, and all of those kinds of people who help advise us on those sorts of things. Clearly we have to define the waterfront, if you will, of information, because we can't process all the information we collect or have access to. So we have to make some judgments about what is important to us, and what is important relative to our theory, and how we want to deal with that theory.

We were talking about structured argument. In this community of interest for competitive analysis, what you want are structured arguments. You want people to come forward with hypotheses and, using the same information, either affirm or deny that a hypothesis is correct, or estimate to what degree it can be correct. That's where we need to go in analysis. We need to look at what the hypotheses are, how we validate them, and then what we do with the ones we validate. How do we continue down that path? Do we collect more information? Do we act on it? What do we do about it?

Oettinger: I hate to break into this excellent conversation, but we're reaching the end of the class time.

Haave: I still have to read my speech!

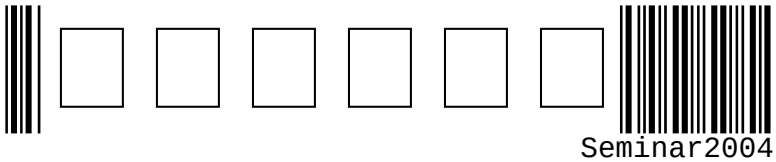
Oettinger: I want to thank you very much for a sparkling and illuminating conversation. We have a small token of our large appreciation.

Haave: Thank you. I expect great things out of you. I'll say this publicly: I'm over the fifty-year mark, and the truth is that I probably have a good twenty years more in me. You have an enormous number of decades to go, and you can make them what you want. You can do very good things. It is very encouraging to see all of you, and I really hope that you do pursue your

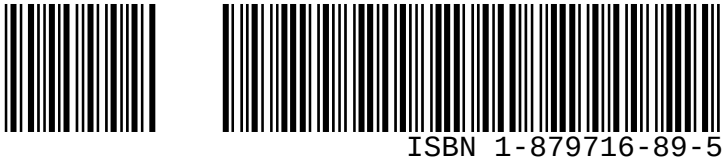
passion. If there's anything I can do to help you, I'm willing to do that. Thank you all. It's really terrific that you're here.

Acronyms

CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
EUCOM	U.S. European Command
FBI	Federal Bureau of Investigation
HUMINT	human intelligence
JCS	Joint Chiefs of Staff
NSA	National Security Agency
OSD	Office of the Secretary of Defense
PLF	parachute landing fall
TIA	Terrorist Information Awareness (formerly Total Information Awareness)
TTIC	Terrorist Threat Integration Center
VSAT	very small aperture terminal
WMD	weapons of mass destruction



Seminar2004



ISBN 1-879716-89-5