*INCIDENTAL PAPER*

# Seminar on Intelligence, Command, and Control

**Challenges Facing the Defense Department in the Twenty-First Century**
**Cheryl J. Roby**

**Guest Presentations, Spring 2001**
C. Kenneth Allard, Cheryl J. Roby, Nicholas Rostow, Richard P. O'Neill, Harry D. Raduege, Jr., Thomas S. Moorman, Jr., Thomas R. Wilson, James M. Simon, Jr., Toshi Yoshihara

**December 2001**

## 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* | *Managing Director* |
| Anthony G. Oettinger | John C. B. LeGates |

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-76-3 **I-01-3**

December 2001

## PROGRAM ON INFORMATION RESOURCES POLICY

**Harvard University** **Center for Information Policy Research**

### Affiliates

Anonymous Startup

AT&T Corp.

Australian Telecommunications Users Group

BellSouth Corp.

The Boeing Company

Booz•Allen & Hamilton, Inc.

Center for Excellence in Education

CIRCIT at RMIT (Australia)

Commission of the European Communities

Critical Path

CyraCom International

DACOM (Korea)

ETRI (Korea)

Fujitsu Research Institute (Japan)

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

Microsoft Corp.

MITRE Corp.

Motorola, Inc.

National Security Research, Inc.

NEC Corp. (Japan)

NEST–Boston

Nippon Telegraph & Telephone Corp. (Japan)

PDS Consulting

PetaData Holdings, Inc.

Research Institute of Telecommunications and Economics (Japan)

Samara Associates

Sonexis

Strategy Assistance Services

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

Upoc

Verizon

**Challenges Facing the Defense Department in the Twenty-First Century**

**Cheryl J. Roby**

**March 8, 2001**

---

*Cheryl J. Roby is deputy assistant secretary of defense [DASD] for programs and evaluation in the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [OASD C3I], a position she has held since January 1999. She began her career in government as a technical analyst for imagery processing and exploitation at the Naval Technical Intelligence Center [NTIC], eventually becoming deputy project manager for a joint Navy–Central Intelligence Agency [CIA] effort to develop a new imagery system, and senior advisor to the NTIC technical director for both imagery exploitation and resource management. She subsequently moved to the Defense Intelligence Agency [DIA]. In 1990 she joined the General Defense Intelligence Program [GDIP] staff as the assistant for collections and served also as the director for program evaluation and operations. In 1991 she moved to the OASD C3I to establish the Intelligence Program Evaluation Directorate of the Intelligence Program Support Office. She became a member of the defense intelligence senior executive service in 1992, when she was selected as assistant deputy director for intelligence program evaluation. In 1993 Ms. Roby was designated director for programs and evaluations in the new C4I [command, control, communications, computers, and intelligence] Integration Support Activity. In March 1996 she became acting principal director for intelligence in the Office of the DASD (Intelligence and Security) [DASD (I&S)]; she was then chosen to fill the position permanently. From June 1996 to April 1998 she was the acting DASD (I&S) and from May 1998 to January 1999 she served as the DASD (I). She earned a B.S. degree in mathematics and is a graduate of the Chief of Naval Operations Advanced Managers Program, the Harvard University John F. Kennedy School of Government, and the Director of Central Intelligence [DCI] Intelligence Fellows Program.*

---

**Oettinger:** I’m happy to introduce today’s guest. You’ve all seen her biography, so I don’t need to go into details about her career, except to note with pleasure that she is an alumna of our executive program. I also want to thank her especially for coming here on such a short notice. We’re delighted that you’re with us, and I turn it over to you.

**Roby:** Thank you very much. I would like to give my presentation today in two parts. I have prepared some formal remarks that I’d like to go ahead and present, because there are some key items and I want to make sure the points are brought to your attention as part of the academic environment that you are working in. Then I’d like to go into some discussion points with you.

One topic that we got into during the lunch period was the organization that I come from, the OASD C3I. I also thought it might be interesting just to talk generally about some of the commissions that are happening in Washington, give you my perspective on where we are in analyzing the data from those commissions, and, I hope, answer some questions that might interest you specifically—on anything that interests you. As I go through the remarks, I'm happy if you want me to stop and we could have a dialogue on some of them, or we could just get through the opening remarks and then get into the question-and-answer part of the presentation, whichever fits best in the environment you're comfortable with here.

As I told everyone at lunch, getting out of the Pentagon is one of the things I enjoy most. It's so hard to get away. The in-box, the activities, and the current emphasis at the Pentagon consume me and many of the people I work with. It's a pleasure to step away from that, to come and see all these bright shining faces, and to think with you. We don't get a chance to think. As sad as that may sound, and as depressing as it may be for some of you to hear me say that, we don't really get a chance to step back from the environment we're working in. It is a pressure cooker. There's a lot expected of us. Many folks work long hours and weekends to try to keep up with the actions and the activities of the Department of Defense [DOD].

Then, I'm always thrilled, intrigued, and a little anxious about the questions. Sometimes I get some zingers, and I have to admit in front of you that I don't have all the answers. I'd like to think I do, based on the position I'm in or the experience that I've had, but I also recognize that's just not possible. There are so many different ways to think about a topic. The environment that you're in right now is fostering that challenging thinking, and I'm thrilled that I'm going to get the chance to hear some of those probing questions. I'll do my best, at least at getting into the right direction to answer some of those.

Right now there's a lot of uncertainty at the Pentagon. In case the news hasn't gotten all the way up to Boston, we do have a secretary of defense, Donald Rumsfeld. We do have a deputy secretary of defense. Paul Wolfowitz has been confirmed and has been sworn in, and he's actually beginning the process of helping the secretary decide who some of the under secretaries are going to be.

There's a lot of bureaucracy and a lot of layering that goes on in the Pentagon. The biggest difficulty this new administration has right now is coming up to speed with the new staff that they want to have. At the moment there are many holes. There have been a few articles in the paper about Secretary Rumsfeld coming to work in the morning and, as he walks into the Pentagon, turning around, looking at the empty parking lot, and saying, " I hope someday, very soon, those slots will all be filled and I can have a number of folks advising me and helping me in this very interesting but yet difficult job."

What I would like to talk to you about today are some of the threats that we're going to be facing in the military, and then I would like to talk about what our new leadership team in the DOD has in mind. Some of these items are going to come specifically from quotations from their confirmation hearings and some of the data that they've passed on to us senior executives. I know that many of you in this room are intelligence professionals, as I am. I think when we get to some of the specific things in the intelligence area they would probably be intriguing and interesting to you, although, again, they are not closed at this point.

> Twelve years ago many observers believed the United States was in a period of permanent decline and pointed to other nations as models for

> reforming the U.S. economy. Budget deficits were taken as a given, the personal computer was a toddler, and the Internet was a mere infant.
>
> In the intervening years, the cold war has become part of history, and we have fought and won a major war in the Persian Gulf. America did not decline, it prospered. We remain a vibrant world power with a position that is in many respects unique in the history of the world.
>
> Under these circumstances, it was only natural that our nation desired to reap a peace dividend. We reduced our defense budget by 40 percent, and cut the force by nearly the same amount. Our defense budget was drawn down to the lowest percentage of our gross domestic product since the late 1930s.
>
> But the world remained, in Secretary Rumsfeld's words, "a dangerous and untidy place." Amidst the peace that encompassed the developed world, ethnic conflicts, regional thugs, failed states, terrorists, and the proliferation of missiles and weapons of mass destruction [WMD] presented new challenges. And the need, indeed the demand, for U.S. leadership increased, as well.
>
> Despite declining defense budgets and shrinking force structure, in the past decade we drastically increased the number of military deployments for humanitarian and peacekeeping operations. This added greatly to the workload of an already busy force, one that was struggling to maintain its combat readiness with dedicated, but tired troops manning aging equipment. Today, as General Shelton has said, the force is "frayed."
>
> We must begin a long overdue renovation and transformation of the armed forces in order to preserve and extend the peace well into the twenty-first century. President Bush has set this task as one of the highest priorities of his administration. As the president has reminded us, peace is not ordained, it is earned; and it must be earned, in particular, by the hard and often dangerous work of our men and women in uniform.[1]

Let me talk about some of the challenges that drive the DOD in our new direction. The first is demographics. We are living in a very dynamic world that is unlike the world in which we operated during the cold war. By 2015, the world population is expected to be 7.2 billion people. Ninety-five percent of the increase will be in developing countries, nearly all of it in rapidly expanding urban areas. Where political systems are brittle, the combination of population growth and urbanization will foster instability.

Another area where we have a major concern is natural resources. We have an ever-increasing need and demand for our natural resources. Overall food production will be adequate to feed the world's growing population, but poor infrastructure and distribution, political

[1] Paul Wolfowitz, prepared statement for his confirmation hearing before the Senate Armed Services Committee, U.S. Senate, 107th Congress, Feb. 27, 2001.

instability, and poverty will lead to malnourishment in many parts of sub-Saharan Africa. The potential for famine will persist in countries with repressive government policies or internal conflicts. Water scarcities and problems with allocation will pose significant challenges to governments in the Middle East, sub-Saharan Africa, South Asia, and northern China. In my estimation, regional tensions over water will be heightened by 2015.

We also have science and technology that are offering us both a challenge and, in some cases, a solution. As George Tenet, the DCI, said in his recent testimony before the Senate Select Committee on Intelligence, "We are in a race with technology itself."[2] Fifteen years ago few predicted the profound impact of the revolution in information technology [IT]. Looking ahead another fifteen years, the world will encounter quantum leaps in IT and in other areas of science and technology. The continuing diffusion of IT and new applications of biotechnology will be at the crest of the wave. IT will be a major building block for international commerce and for empowering nonstate actors. Most experts agree that the IT revolution represents the most significant global transformation since the industrial revolution that began in the mid-eighteenth century. Disaffected states, terrorists, proliferators, narco traffickers, and organized crime are all going to take advantage of the high-speed information environment and other advances in technology and integrate them into their illegal activities. That will compound the threat to the United States.

We know that the possibility is greater than ever that the revolution in science and technology will improve the global quality of life. What we have to deal with now is very exciting. The advances are helping us break through in various areas. However, what we don't know about science and technology is just as staggering. We do not know to what extent technology will benefit or further disadvantage disaffected national populations or alienate ethnic and religious groups or the less developed countries. We do not know to what degree lateral, or what we've called "sidewise," technology will increase the threat from low-technology countries and groups.

One certainty is that the progression will not be linear. Another is that, as future technologies emerge, people will lack full awareness of the wider economic, environmental, cultural, legal, and moral implications. We will also have the potential to continue research and development and try to impose those technologies on underdeveloped countries.

One of the serious concerns that we have right now regarding our national security is our reliance on IT. The computer systems that we have and the way we apply our weapons technology all rely on the IT revolution. Our weapons systems become ineffective if we don't get the right information to the right person at the right time in the right format. We are very seriously challenged by this revolution.

One of the other areas that we are very concerned about, and where we think we will have very serious conflicts in the future, is WMD. We already know about Russia and China, but, more likely, we're going to be facing the North Koreans, probably the Iranians, and even Iraq in this venue. Our concern is how we are going to deal with that and keep from putting ourselves at risk from these countries with their use of WMD. When I use that term, I don't mean only nuclear weapons. We are very concerned about and putting a lot of energy and attention on biological and chemical weapons as WMD.

[2] George J. Tenet, "Worldwide Threat 2001: National Security in a Changing World," testimony before the Senate Select Committee on Intelligence, U.S. Senate, 107th Congress, Feb. 7, 2001.

One of the things I want to spend a little bit more time on is something that you probably have heard referred to by other speakers, and that's asymmetric warfare.[3] Most adversaries recognize that the information advantage and the military superiority of the United States are here now and are going to continue as we go into the future. We recognize that developing countries are seeing that as a vulnerability as well, and that they will try to circumvent or minimize our strength by exploiting our weaknesses.

IT-driven globalization will significantly increase interaction among terrorists, narco traffickers, weapons proliferators, and organized criminals, who, in a networked world, will have greater access to information, technology, finance, sophisticated deception and denial techniques, and one another. Such asymmetric approaches, whether undertaken by state or nonstate actors, will become the dominant characteristic of most threats that we fear to the U.S. homeland. They will define a challenge to U.S. strategy, operations, and force development, and they will require that we use a strategy to maintain our traditional superiority. We would like to consider their threats low and not have them pose a serious problem for us, as we have to deal with and harness the potential that they bring. At the same time, we do not know the extent to which adversaries, whether they're state or nonstate actors, might be influenced or deterred by other geopolitical, economic, technological, or diplomatic factors in 2015. If anything, we don't think that they're going to be scared off by any of those factors. Many of the terrorists, traffickers, and even the criminal element are not concerned about morals or anything that would hold them back from making the United States a target of destruction, and we fear what they would do.

Let me now jump into what the president has said and what he expects of us in order to counter what I've quickly laid out for you as some of the challenges. The president recognizes that the DOD should concentrate on three important goals. First and foremost from the president's perspective is that

> …we must strengthen the bond of trust between the American people and the military. As [Army Chief of Staff] General Creighton Abrams said when the All-Volunteer Force was first created, "people aren't *in* the Army. people *are* the Army"—and the same is true of all the military services.
>
> Building on the dedicated work of the House and Senate, we must continue to improve military pay and quality of life. But good pay and fair allowances by themselves won't keep the best people in the service. Working with the Congress and with our allies, we must also reexamine the balance among force levels, commitments, and deployments. We will have to make sure that we are focused on the most important defense tasks and not placing unreasonable demands on our men and women in uniform.
>
> We will also have to acknowledge the relationship between morale and readiness. President Bush has said that "even the highest morale is eventually undermined by back-to-back deployments, poor pay, shortage of spare parts, bad equipment, and rapidly declining readiness." Our men

[3] See Thomas R. Wilson, "Asymmetric Approaches to Joint Vision 2020," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, November 2001), [On-line]. URL: http:www.pirp.harvard.edu/pubs.html

> and women in uniform must have first-class equipment, adequate materiel for training and maintenance, decent barracks, modern family quarters, and suitable working conditions.[4]

**Student:** I'd like to go back for a second. How do we go about building this trust? Maybe some of that would come about through cuts in personnel. If we do cut personnel, maybe we all of a sudden will have more money to make these things possible, but what happens to morale when we're closing bases or taking out a carrier?

**Roby:** One of the things that I was going to get to, but we can talk about it now, is the defense strategy. Right now within the DOD we are looking at what a new strategy for the department might be. We are currently operating under the two MRCs—major regional conflicts—strategy. The question is, is that the right strategy to have? There are many who believe it needs to be revised, and that we don't have the full capability to fight two major regional wars, so we should acknowledge that and build a strategy that we have the capability to execute.

We're expecting the secretary of defense will need forty-five days to complete this defense strategy. Secretary Rumsfeld will lay that out for the president and say, "Okay, here are the things we're going to have to do." In there, he will probably have to decide how he is going to accommodate the items I was talking about. We've already gotten the pay taken care of. The pay is in the budget now, so we have improved the salaries associated with our military folks. It doesn't improve the salaries as much as maybe some would want, but it is a significant step in the right direction. It didn't do anything significant for the pay of DOD civilians. We also recognize that the facilities that we have allowed to erode have got to be improved, and there is already some money for improving facilities in the president's budget that we just submitted.

The basic answer to your question is that Secretary Rumsfeld is going to have to decide what exactly he wants to lay in front of the president. It could be, "Don't cut anything in terms of people; just put in new money above the current dollars that you have allocated for the Defense Department." You might recall that in the Reagan days we had a $400-plus billion Defense Department budget. Right now we're at $310 billion, so it is not impossible to have the secretary of defense go forward with a recommendation that increases the budget overall without having reduced the number of individuals we currently have on the books.

When he has finished his strategy, the secretary of defense will look at it and decide, "Is that worthwhile? Is it appropriate? Can we achieve it? Do I want to make this the means by which I do exactly what I said in my first statement? I gain the trust and a bond, effectively, with the military. Then, do I move on from there with revamping the force structure? Will the military departments agree that it may not be necessary to have ten divisions for the Army, or eleven aircraft carriers for the Navy? Will they agree that force structure should be modified, and actually reduce the force structure?" If we get to that point, and there is a decision, then the impact will be to look at the force structure in terms of people and decide whether those people would not be retained or whether we would just do this over a period of ten years. There's also a possibility that we might decide that we won't release anyone, we just won't hire any new people. We'll put a freeze on hiring and maybe a freeze on some of the recruiting that's going on. I'm not good enough to know exactly how the secretary's going to tee that up for the president for his final decision.

[4] See note 1.

**Student:** You mentioned internal issues of trust and morale. Is the DOD preparing to address external issues such as the effect on morale of the lack of respect and/or knowledge about the military among the U.S. public?

**Roby:** Yes. That is one of the key tenets that Secretary Rumsfeld expressed in his comments about the civilians on board the submarine when we had the tragic crash with the Japanese.[5] He said that from his perspective it's still imperative to have public exposure to what the military does, how it does it, and why it does it. I think that will become part of a campaign plan, if you will forgive my use of the term, and part of his defense strategy. I believe Secretary Rumsfeld feels that very strongly. I think that with a background like his—having been secretary of defense in the 1970s, having stepped away from the DOD, gone off and run a major pharmaceutical company, and then come back to the DOD—he would support more outreach and more activities that give the American public better knowledge and understanding of what the forces do and, therefore, what the dollars that come out of their taxes are being used for.

I'll go back really quickly to two more items from President Bush, and then we'll go on with some of the general comments. The president wants us to develop capabilities to defend against missiles, terrorists, and complex sets of threats to our information systems and to our all-important assets in space. The reason I wanted to make sure I made that point to you is that I want to highlight for you what's been happening with the Space Commission.[6] One of the activities that Secretary Rumsfeld was involved in before he was selected to become the secretary of defense was serving as the chairman of a commission looking at what we do today with our space assets and what improvements it would recommend to the president and whoever might be the secretary of defense. Lo and behold, he now has finished the report, and he's producing it and giving it to himself.

It's a rare occurrence, I might add. I don't believe I've ever experienced anything like that in my years in this job. Typically, a commission report comes in and folks look at it, find a couple of nuggets, and say: "Those look like good ideas and we'll get to them." We all recognize that is not what's going to happen this time, because the secretary of defense, when he was part of the Space Commission, actually saw, wrote, approved, anointed (whatever term you want to use) all of the words that were sent forward to us. We think we're going to be doing something associated with it.

Let me highlight a couple of the items that Secretary Rumsfeld wanted done when he was part of the Space Commission. He very much wanted to build rapport and a very effective relationship between the secretary of defense and the DCI. One of the things that has happened over the years is that they have both become, in a way, cabinet members, but with their own agendas and their own expectations. Secretary Rumsfeld's Space Commission felt it was ineffective for the government not to have them totally aligned and working toward a common purpose. Therefore, one of the things that is highlighted is to build a relationship between them.

[5] The U.S. submarine *Greeneville* collided with and sank a Japanese fishing vessel, the *Ehime-Maru*, on Feb. 9, 2001, while the submarine was taking civilians on a demonstration trip.

[6] For a discussion of the so-called Rumsfeld Space Commission, see Thomas S. Moorman, Jr., "The Commission to Assess U.S. National Security Space Management and Organization," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, November 2001), [On-line]. URL: http:www.pirp.harvard.edu/pubs.html

They have done that already. The secretary of defense and the DCI have weekly breakfasts. Sometimes the meeting gets moved to later in the day. The agenda is varied. They talk about substantive intelligence some of the time. They discuss current world affairs, what's happening, what some of the information flows are that help us in analyzing this current situation, what some of the gaps in information are, and whether intelligence can help in filling some of those gaps. They have a very good rapport with each other as they look at those: "What can I, the DCI, do?" "What can I, the secretary of defense, do?"

In addition, Secretary Rumsfeld's Space Commission agreed that we really need to have improved emphasis on space within the DOD. Yes, we do understand space is important, and we have used space in a multitude of venues: intelligence gathering, weather, navigation, and many other areas. The DOD agrees with the Space Commission that it is important to highlight the benefits to be accrued from emphasis on space so that everyone understands them. In that vein, the DOD is working to provide explicit guidance to the DOD elements for objectives, priorities, and programs that need to be accomplished within the space venue. That's different. The DOD has never provided this level of guidance before, and it's going to be an interesting challenge to see just how far the DOD can go.

Many of you who are in the military realize you've got to find a balance. You can't take one business area, place it above all others, and be successful. You've got to ensure that you are creating a balance among all the mission areas. There is a little concern that we may be putting too much emphasis on this business area, or this mission area, at this time. We'll have to see how that unfolds.

We expect the secretary will make his final decisions by mid-April. Once he's decided what he accepts of the Space Commission's recommendations he'll bring them forward to the president, have the president endorse his recommendations, and then, as is the case in at least two areas of the recommendations, we have to get Congress to endorse what we want done.

One of the two areas that require congressional action is authorizing us to have an additional under secretary of defense. Right now, we're limited by law to four, and what they're talking about doing is creating a fifth. That fifth would have space, information, and intelligence as his or her responsibilities. We expect that person would be using the basic organization I come from—the OASD C3I—as the core and elevating that organization to an under secretary position.

The other area in which we need authorization from the Congress is the number of assistant secretaries. If you elevate the under secretary and decide you want to have assistant secretaries working for the under secretary, you need that approved by Congress as well.

The Space Commission's report is open. It's unclassified. Amazing as that may sound to some of you (and especially to me) in a business where even talking about space was classified in the past, it's on the Web. You can call it up and read the entire report.[7]

The Space Commission talked about creating an Office of Strategic Reconnaissance [OSR]. In the old days, we had a skunk works, if you will (my term, not theirs)—a capability really to take a business area like space; put a small, technically competent group of people together; and allow them to develop, launch, manage, and operate that capability. They were autonomous from all the other rigors and the bureaucracy of the Defense Department. You may remember that's

[7] See Report of the Commission to Assess United States National Security Space Management and Organization, [On-line]. URL: http://www.defenselink.mil/pubs/space20010111.html

how the U-2 and the SR-71 were born. What the Space Commission recommends is that we go back to that for at least some aspects of our needs in the space arena. Looking at maybe setting up an Office of Strategic Reconnaissance might add value. We do not have any idea whether the secretary thinks that would be useful and whether he would want to proceed with that.

**Student:** What’s the reaction of the NRO [National Reconnaissance Office] to this?

**Roby:** If it’s within the NRO, good idea. If it’s going to be separate and distinct from the NRO, we really need to decide what its job would be and how it would perform it. I do understand their concern. Would we take people away from the NRO to establish the cadre of technically capable, competent people in this new office? They’ve got the most experience. They’ve got the talent. They’ve got engineers who have really wowed us with the capabilities they’ve developed. The answer: Probably. Well, then, are we going to erode the ability of the NRO to continue providing us the needed sources of space intelligence? I think that’s the dilemma that they’re facing. We just don’t know what the secretary will decide. He might decide that he will allow this to be stood up, but within the NRO. It is not clear at this time.

**Student:** And the money?

**Roby:** That is very much a concern for all of us, particularly for the NRO. If, as I described earlier, new dollars are established in the Defense Department, first and foremost on the list, I would expect, would be the Office of Strategic Reconnaissance. We’re hoping that would be the case, for the same reason. If the NRO is still going to be obligated to deliver on the missions and functions that it currently has within the dollars it’s given, it’s going to become difficult for them to achieve if we take away any portion of that funding. The concern would be new money being brought to a new organization or new money brought to the NRO, rather than money out of the NRO’s existing budgets. Those of you who are experienced in the budget arena recognize this as a very contentious issue.

To switch gears just for a quick second, the president hasn’t exactly established all of the backing he needs for getting the final deliberations from the Hill on his tax plan, on account of tax reduction and so on. This would add to that equation.

I don’t have a good answer for you. We may end up delaying any final decisions until we build a new president’s budget. We just sent the president’s budget to the Hill on February 28. We are still in the throes of finalizing that budget so that it is characterized by President Bush’s priorities. It was built when President Clinton was still in office, and we have not had the opportunity to revamp it to reflect the priorities of Secretary Rumsfeld and President Bush, because we’re still deliberating on what the priorities would translate into in dollars and people. We’re just not there yet. We expect we will have to clean that up thoroughly within a month or two and be able to tie the dollars that we have to details of the priorities for those expenditures. If I had to tell you right now how to spend the money I’d be telling you how President Clinton had told us how to spend the money.

**Oettinger:** I’m forming the impression that your most recent remarks kind of take away some of the things you had given in the comment about Rumsfeld being unique in handing himself the report. If I hear it correctly, a report-writing chairman can be a gadfly, but he doesn’t have to live with the budget. The secretary of defense has to defend a budget that has a constituency. It seems to me that your latest remarks suggest that the reality of incumbency may outweigh anything that is gained by Rumsfeld’s having chaired the Space Commission.

**Roby:** That would be my reality check to all of you: where you stand is where you sit, as many people often say. Secretary Rumsfeld, as a chairman of this commission, may have had grand plans for some other secretary to implement. Now that he has to implement them, he may not do so. That’s why I was saying “expect.” In a circumstance where implementing the recommendations is a policy decision, where it’s a reallocation within his existing responsibilities that he feels very strongly about and he doesn’t need the Congress to agree, it would be my guess that it would be easy and he would follow through. On recommendations where he needs more money or he needs the Congress, he may say: “Not this year. Let me wait until I have a little more time, until I finish the defense strategy, and I can put it together as a complete package.”

I’m just not clear at this point exactly how he wants to proceed, which is why I gave the caveat. We are working diligently every day on assessing and characterizing the impacts of option A, option B, and option C associated with each of the recommendations in the Commission’s report so that we can give the secretary some sense of what the reality means now that he actually has to make a decision. How do you make the bureaucracy of the Pentagon accomplish these items that sounded good when you put them on a sheet of paper? Now that you actually have to churn within the department, what would be affected? How do you actually establish a new organization? How do you actually make a budget appear for something called space? Where would you have to take it from if you did it internally? Where could you go to ask for new money, the Office of Management and Budget or the president?

**Student:** I was going to ask about the new relationship between Secretary Rumsfeld and Mr. Tenet. Are you talking about relevelling OSR and NRO, or are you going to throw NIMA [National Imagery and Mapping Agency] and NMD [national missile defense] in there, too, and put that into the space mix?

**Roby:** NMD is in the mix, because we expect there to be certain information that will help accomplish the NMD mission—Star Wars, to use the Reagan parlance. It needs space to be successful. What needs to be teed up are things such as: What are the capabilities for NMD? Which NMD do you mean? What capabilities and over what timelines? Do you want an accelerated NMD? Do you want an elongated one? If you can give us those, Mr. Secretary and Mr. President, we can tee up for you what we have planned and programmed today, and it will deliver *this* capability by *this* date. Then we can say, “If you want this, for instance an accelerated date, here’s what it will cost in programs, here’s what it will cost in dollars. You need to make the judgment on that.”

NIMA has to process the data that come from the system, so it’s also very much in the mix when you talk about improving our space capabilities. It doesn’t do us any good to add satellite capabilities for which we are unable to process, exploit, and disseminate the data.

**Oettinger:** It’s fair to say that’s exactly what we’ve been doing for the last couple of decades, so the notion that such a stupidity might continue is not ruled out.

**Roby:** To the extent that we have done that, some would argue that you cannot bring a satellite down, add capability, and then put it back up when a surge or a crisis occurs. Therefore, you build to the max and give yourself the opportunity to surge on the ground when you need the data rather than leave yourselves with no ability to have that information. There are some who say "One for the burn bag, one for the light table" could have been logical, because maybe they're won't use that burn bag when they're in a conflict situation of some kind.

**Oettinger:** As long as we're in a provocative vein, can I take you back to your comments about asymmetric warfare? Let me preface my question with a remark about the cold war, where we got into the habit of scaring everybody to death over what used to be known as the "ten-foot-tall Russian" who, it later turned out, didn't exist. I'm wondering whether we're doing something similar with the "ten-foot-tall terrorist."

Let me put it in an exaggerated way. We can't keep a high school student from going to the high school and shooting at people. The odds of keeping Osama bin Laden or anybody else from doing something random are about as good as stopping some suicidal presidential assassin, which we've seen from time to time. First of all, is that a sensible statement to make or just a stupidity? If it's not all that stupid, then where is the boundary between unavoidable tragedies, which are terrible for those who happen to be at the receiving end of the bullet but which make no difference as far as the total social fabric or the survival of the United States is concerned, and something that is a strategic threat? I'm just wondering whether we've drawn the right boundaries in focusing on asymmetric warfare.

**Roby:** My answer would be that we are still trying to decide exactly what level of emphasis we're going to put on it, but we're raising everyone's consciousness that it's not just nuclear war that we need to be prepared for. We, the United States, and then we, the military, have a changed environment.

**Oettinger:** But the notion of the one nuclear weapon coming in on a truck is a similar kind of thing, so this asymmetric question arises with every kind of weapon. I don't see what to my taste would be enough thinking about the level at which we will take it seriously and the level at which it becomes sort of mission impossible in a country that, after all, tolerates annual road kill far greater than anything that happens in any kind of terrorist or military situation. We only impose speed limits and then ignore them.

**Roby:** What we've been trying to do with our seniors and then with the Congress and everyone else is ask where the boundaries are at which we will feel we have done the most we can in a defensive and offensive approach to this problem. Have we looked at our networks, for example. As I described earlier, we have an IT splurge. We are using it in every vein. Are our networks protected? Have we put enough energy into looking at them, and then dollars so that we have defense in depth when we look across our infrastructure?"

I will tell you that our office will declare, "No. We have not done enough." We have brought more visibility to the fact that the critical infrastructure of the Defense Department is a byproduct of our using open, available infrastructure—power lines, land lines, water— about 95 percent of the time. That is what feeds our military departments here, and when we go abroad it's even more true. We rely on that critical infrastructure. One of the things that we have been looking at is how we would protect our critical infrastructure. If one of our adversaries thinks through an asymmetric threat, is there anything we can do about it, or do we just throw up our hands and say, "Too hard, too big. We're just going to walk away from that problem"?

That’s the kind of dialogue that’s going on and will go on, especially as we decide the defense strategy. They’re going to have to wrestle with this idea and answer the question that you posed: How much can we do anything about, and how much should we attempt to do something about with respect to anticipating, expecting, dealing with, and understanding asymmetric threats? Some would tell you we’ve had asymmetric threats from the beginning. They are nothing new. All adversaries always had the opportunity to do anything they wanted to hurt the United States, and you could call that an asymmetric threat. If you looked at the situation in that vein, they didn’t ever actually have to go force on force.

**Oettinger:** During the cold war the question was poisoning the water supplies.

**Roby:** Exactly. This has been thought of before.

**Student:** Isn’t there another element in the consideration of asymmetrical threats beyond just “Can we do anything to prevent it?” There’s also the aspect that once it occurs we have to have some rational way of dealing with it and reacting to it. What is our recourse going to be after it has occurred? I understand you’re saying we can’t predict. I know you would say that without meaning to state an absolute and saying, “We can’t do anything about it, so why worry about it.” Even if you can’t do anything about it, you still have to figure out what we are going to do in reaction if it occurs, and whom we are going to react against. “Do I even understand that it occurred to begin with, and who are these folks?”

**Oettinger:** I was watching a news story yesterday about the California state police revising its tactics because they realized that sending in SWAT [special weapons and tactics] teams who were trained for hostage situations is not the way to control a situation in a high school when you want to get in there really quickly and stop the shooting as opposed to getting in there late and disabling or killing a perpetrator. Some of you may have been exposed to meetings here in the Kennedy School about the problem of controlling the swine flu, where, in a fit of good intentions, we provided vaccines whose side effects were much worse than anything that might have occurred in the epidemic. This notion that somehow every threat has a remedy and is worth devoting resources to raises its own problems. We succeeded in bankrupting the Russians by virtue of the Star Wars theater being thought real by them, and I worry about flipping this asymmetric threat thing around to bankrupt us in chasing a phantom. I’m not reaching a conclusion on that, mind you. I’m just raising that question in a context where our guest brought up the asymmetric threat question. Let’s examine it a bit.

**Roby:** I think the question is very important. We are trying to exercise so folks get more comfortable and more familiar with the potential paths we could follow after an action taken by one of our adversaries. That is opposed to the exercises of old, which were very narrowly focused on just looking at what would happen if the Russians came through the Fulda Gap, or repeating the Persian Gulf war or North Korea coming across the DMZ [demilitarized zone]. We’re starting to get to a point where the scenarios are much more hypothetical, but along the lines of what you were just talking about. What would we do if the blood supply of the DOD were tainted? Is that an asymmetric threat? Well, we would kind of put it in that category. What would we end up doing? We can’t deploy. We can’t fight. Those are difficult situations for which we have to consider how we could recoup from them quickly and do exactly what you said. We’ve got to think about them in the context of “This happened. What are we going to do to regroup?”

We've got to get the seniors—"seniors," as in "cabinet members"—to sit around tables like this. This is not going to be done by the Defense Department. That's where I was headed with the mention of critical infrastructure, which is neither unique to the Defense Department nor something we should be trying to protect unilaterally. We should not be in the lead, nor should we be the only ones trying to work on critical infrastructure protection or information assurance. That's something we need to do as a whole government.

We also have to work with our allies. We have to define and build the relationships to establish what they are going to do and what we are going to do. As you are well aware, the weakest link in the chain is where you're going to fall apart as you go into any situation, so we want to make sure that our allies are well aware of and doing things about those situations early enough so that we do not have that problem in a conflict or even a humanitarian or peacekeeping operation. We would still have to ensure that it was taken care of.

**Student:** I assume Dick Clarke is still sitting up there as the guru of critical infrastructure.[8]

**Roby:** Interestingly, he is now focusing more on the cyber side and a little less on critical infrastructure and terrorism.

**Student:** I worked on that before I came here, and the reason he did that was that the rest was just too big. Cyber was big enough, so people thought, "Let's just go to cyber and figure that one out, and we'll be fine."

Where I'm heading with this is that at least a third of us in this room are anxiously awaiting the national security strategy, which we expect to be put out in May or June, or whenever Dr. [Condoleeza] Rice manages to figure out exactly what she wants to say and gets the president to buy off on it. To do that more effectively, this administration needs a radical change in the formal NSC [National Security Council]—not the staff, but the formal, original NSC. Are you seeing Secretary Rumsfeld and Secretary Powell going back to the old Eisenhower NSC, where they actually do meet and have position papers and discuss policies?

**Roby:** Absolutely. They are to include 42 people in the NSC now, as opposed to 142 in the previous administration.

**Student:** That's a major reorganization.

**Roby:** Major events are going on, and they are doing exactly what you said. They're having it teed up so that we're really talking about a small group—about Colin Powell and Donald Rumsfeld and Condoleeza Rice and the president in meetings where they're really trying to push agenda items and make decisions, and then taking those decisions and proliferating them. However, they're very restrictive and very close on what they're working on and what details they want to flow, much more so than we saw in the previous administration, where a lot was tested or reviewed before. That is not the approach that they're taking. They're keeping it to themselves, and so it's exactly what you just suggested.

**Student:** It's not that anybody is saying anything. In fact, most people are saying, "We're not going to talk about it."

[8] In October 2001, Richard A. Clarke was named special advisor to the president for cyberspace security. In the Clinton administration, he had served as the National Security Council's coordinator for critical infrastructure protection.

**Roby:** We get very little guidance or things we could quote as “This is the guide, this is the plan,” but we do know that both the defense strategy and the national strategy (you start with the national strategy and from there you go to the defense strategy) are in process at this point.

**Oettinger:** Think balances. Been there, done that. Nixon’s administration did a similar kind of thing and promulgated things out of a closed circle. It hit a bureaucracy that hadn’t been informed and hadn’t been involved, and the stuff essentially sank like water into dry sand. Where do you strike a balance between this closely held, dynamic decisionmaking and then screwing up the implementation versus slowing down the implementation by having testbeds where you get the edges burned off? Maybe then it’ll die, but maybe if and when the decision is made, people are prepared to do it and there’s a reason. It’s a hard problem.

**Roby:** Very hard, because you can go the other way. If you allow it to start at the grassroots level and then go to various other places, it could be talked to death prior to being brought to the seniors’ attention, and there are plenty of doors where it would have to stop just in the Pentagon before it could get teed up for the secretary of defense. You could actually end up with no progress being made toward the very serious and potentially contentious policy decisions that need to be made.

You’ve called it correctly. It’s got to be a balance, and you’ve got to have confidence in the seniors you have to implement the decisions. That’s the dilemma we’re facing right now. There aren’t any seniors available within the Defense Department as of this date. We expect to have the comptroller nomination shortly. The intent was sent last Friday. We expect to hear by this Friday that the actual nomination of Dov Zakheim as the comptroller was sent to Congress. That will start the process. Then, we believe, we’ll get the nominations very quickly for under secretaries of personnel and readiness, policy, acquisition and technology, and logistics. Those are the four under secretaries who really support the secretary of defense.

To answer your question, Tony, what we believe is that Secretary Rumsfeld has confidence that these folks can make things happen. We expect he would turn to them and direct them to do something, and then they’re going to have to build their implementers—the lieutenants and the captains and the majors—and say, “Okay, the boss said *this*. Now, let’s get it done. Let’s find out what the barriers are and let’s get them get them out of the way, because we need to close on this quickly.” We’ll watch as that one unfolds, because I think it is going to be very interesting for a lot of us.

They also have to deal with the NIMA Commission, the NRO Commission, and the Hart–Rudman Commission. NIMA and NRO are along the lines of what I was I was saying about the Space Commission, although they were not chaired by Rumsfeld. Congressman Porter Goss [Rep.-Fla.] chaired the NRO Commission and Peter Marino[9] and [General Sidney] Weinstein and several folks like that were on the NIMA Commission.

For the NRO, the expectations are that in order for us to be successful in the future, we’ve got to get back to basics. We’ve got to get them on track with being able to deliver advances in

[9] Peter Marino, an entrepreneur and technologist, has served with the U.S. government in a number of high-level national security roles. He currently co chairs the Defense Science Board Task Force on Intelligence Needs for Homeland Defense.

capabilities. They're doing a great job. We have no complaints about the job, but they're not producing the advances that we need.[10]

On the other side, NIMA's struggling. It's a new organization, just stood up in 1996, still getting its sea legs, and still working to get the right cadre of people to do a necessary job. They've got to acquire a very expensive, complex, difficult system to match the satellite systems we were talking about, and they don't have the technologists on board within NIMA to meet that challenge. They know it. They're trying to fix it. They've asked for our help in the Office of the Secretary of Defense [OSD] and they've asked for help from the DCI. We are helping them by giving them new allotments for hiring at the level of seniority for those positions that would help attract the best and the brightest from private industry into the government to do these jobs, because we really do think an infusion of acquisition expertise is an imperative. That is the only way that NIMA is going to be successful with where it wants to go.[11]

The other big factor in all three of the commissions is commercial imagery. We need to take full advantage within the government of what industry is already doing for the nation at large, of the industrial base that's capturing imagery for the global environment, rather than creating government-furnished kinds of capabilities. We're looking for NRO and NIMA to come forward with the best strategy for taking advantage of commercial imagery.

The biggest drawback to doing that is that commercial imaging has got to be successful, and the track record is somewhat lacking at this moment. They have not had as many successful launches of the new capabilities as they would have liked. Again, we are looking to back them, to take advantage of private industry, and do industrial outsourcing of commercial imagery when it becomes available. That's another tough balancing act. Can I count on their being there? Can I count on their not giving the same product to my adversaries? Those are all part of the licensing agreements that we have for commercial U.S. vendors that we could put in place. We don't have similar restrictions on non-U.S. vendors of commercial imagery. They're not successful as yet either.

**Oettinger:** Why not privatize all U.S. space assets and sell the products at prices that undercut everybody else's?

**Roby:** That has been discussed many, many times. There's a fear factor. Will the government continue to deliver on that promise, or will the government step away from that agreement when it decides it's not in the government's best interest?

**Student:** Do you mean a fear factor from overseas that the U.S. government will renege?

**Roby:** Also from private industry folks, who are saying, "If we get into the mode where we're going to do our agricultural assessments or look for oil or whatever and we're going to rely on government assets to determine where we will invest our capital, what happens if the government doesn't deliver or doesn't allow us to have those assets or puts restrictions on them? Can we get a commitment that the government is going to follow through? We're not sure, so we'll go ahead

[10] See Report of the National Commission for the Review of the National Reconnaissance Office, [On-line]. URL: http://www.fas.org/irp/nro/commission.htm

[11] See The Information Edge: Imagery Intelligence and Geospatial Information in an Evolving National Security Environment, Report of the Independent Commission on the National Imagery and Mapping Agency, [On-line]. URL: http://www.nimacommission.com.htm

and back Space Imaging or Earthwatch with commercial venture capital. We know that they're out for profit."

Government's not out for profit. It hasn't been in the past. I should place a caveat on all of those. It has not been, to date, the path we have been on. As we build our national strategy, as we build our defense strategy, these are all issues that need to be considered as part of the new administration's perspectives on what they think needs to be done.

**Oettinger:** If I may emphasize a point, there is also a significant tradeoff between technology and policy. Let me give you one example, but it is important to look for others. This comes out of the financial services industry. All of you are aware of the hoo-hah over using credit cards over the Internet. Big fears, blah, blah, blah. Then it finally dawned on people that it was a problem that had been solved long ago by policy fiat, when the credit card industry agreed on a $50 liability limit per credit card, which makes all of you relax about giving your credit cards to a waiter in some sleazeball restaurant. You don't give it a second thought, because you're protected beyond $50. It's the same thing on the Internet, and the odds of running across greater sleaze on the Internet than in some restaurant are minimal.

Seriously, there are tradeoffs between a policy decision to accept the liability level, for example, and having to find some cryptographic, technical solution—which nobody has found yet—to maintain adequate security for your credit card number as it travels over the Internet. My guess is that in the defense realm there are many such tradeoffs where a policy innovation could make a vast difference in the amount of dollars spent on various things in a classical way.

**Roby:** There is also an expectation by private industry that they're going to make a significant profit with commercial imagery. Giving up that profit, when they felt the business case had been made and venture capital was available, was another reason not to want to have the government go into the business. "Leave it to us. We will do this and we have a market. We have convinced ourselves we have a U.S. market, but we've also convinced ourselves we have a global market for commercial imagery. Don't take that away from us." That was another reason why, in these economic debates about benefit to the U.S. citizens, we convinced ourselves that we should let private industry try, see how far they get, and see how successful they are.

**Student:** Last week we had a speaker in from the CIA, who said that the reason why the agency hasn't really pushed the envelope on technology was because of the concern over protecting it—security to ensure that only the people who are allowed to see things actually see them.[12] However, you told us something completely different here. You said that at the DOD it's basically the other way around. You're pushing the envelope on the technology side and there are serious security concerns that need to be addressed. It's pretty much 180 degrees from what the speaker said last week. My question is twofold. First, how do you balance protecting the infrastructure against pushing the envelope, and, second, why isn't there a kind of standardized policy on this for the entire intelligence community, given that the CIA, DIA, and ASD C3I are all pretty much in the same boat here?

**Roby:** I need to get us back together. When I'm talking about the use by the United States, we want a global, secure, interoperable infrastructure. It's called the Global Information Grid, and the

[12] See Carmen A. Medina, "Intelligence Analysis in the Twenty-First Century: Reaching for Higher Ground," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, 2001), [forthcoming].

DOD has worked cooperatively with the CIA to become a partner/player in this secure infrastructure.

We don't generate the power to run that grid. That's the part that I was trying to get to. We can have a wire, and the wire itself could be impermeable, but there are pieces of the infrastructure that we don't own, such as the telephone line that we're going to run on. Yes, there may be some that we buy uniquely that go from point to point, but beyond that, unless we're going to wire the entire world with our own secure network, we're not going to get there. Neither is the CIA. They have certain point-to-points that they can control, but there are others where they have to rely on the general infrastructure to get where they want to go.

We have put policies in place. If organizations want to play with the Defense Department, they are to follow those policies. They've been promulgated within the DOD over the last eighteen months. We are still working through all the standards to go with those policies. That's the hard part. It's easy for us to write a document. We do it all the time. The hard part is actually making it work. We can set a policy, and we can send an implementation to go with the policy. What we need is a standard, so that everybody is able to do it. We have a joint technical architecture that tells people what the boxes that they've got to build need to look like. Now we're working on standards for this Global Information Grid. What standards is it going to have to adhere to so we can sustain secure communications to the maximum extent possible?

Certain networks are not open. They don't connect to the Internet. They don't connect to the SIPRNet [Secret Internet Protocol Router Network], our secret network. Administrators of those networks are much more confident that they're secure, that no one can intrude on them, but you can never stop the insider, and we proved that with the FBI agent who's just been arrested.[13] There is a vulnerability in terms of tapping into those networks that we have to recognize and do something about, but we still have the power problem. In some places we generate our own power, but not everywhere.

That's what I was headed for on the other point, that we need to get into a mode of recognizing where the vulnerabilities are. Can we do something about them? As Tony said earlier, with some of them you just have to just say, "Nope, can't do anything about it. What's the work-around?" As someone else said, "Run through some exercise that says, 'Okay, if I lose *these* data, I'm going to find *those* data and I'm going to send them.'" Our bottom line is that you've got to get the right data to the right person in the right format at the right time, or you're useless. You can't accomplish your mission if you haven't made that one of your primary objectives prior to engaging in humanitarian operations, peacekeeping, conflict, or whatever it may be.

That's what we are trying to get everybody to recognize. Not everybody does, I might add. We're still working to get all the cabinet members to understand what we're talking about. A lot of them look at this as a defense problem. "Make the Defense Department spend their money to make this happen. Their job is ensuring that problems don't occur. Isn't that their job?" We have to stop them and say, "No, that's not exactly the right definition of the job of the Defense Department."

The Hart–Rudman report on homeland defense has recently gone over to the Hill.[14] Who is responsible for homeland defense? Should we establish a homeland defense agency? Should we

[13] In February 2001, Robert Phillip Hanssen was arrested and indicted for espionage.

[14] The U.S. Commission on National Security/21st Century, better known as the Hart–Rudman Commission, cochaired by former senators Gary Hart (Dem.-Colo.) and Warren Rudman (Rep.-N.H.), released its Phase III report on

start a new organization whose job, end to end, would be to work homeland defense, and that would have the FEMA [Federal Emergency Management Agency], the FBI [Federal Bureau of Investigation], Defense, and other elements of the cabinet feeding into this agency? The jury is still out on that. You may solve some things by establishing an agency for homeland defense, but you also add a tremendous amount of complexity in terms of how that organization will operate in our environment.[15]

**Oettinger:** Talk about trust building between those groups! The financial services industry, for example, with which I was intimately familiar during the period of the President's Commission on Critical Infrastructure Protection, doesn't want anything to do with any part of the government.

**Roby:** We're still having difficulties. One of the things we have tried to convince industry of is the vulnerability of networks. When we find some kind of a problem in a Microsoft network and we know about it, we want to share that problem. Microsoft wants to know so they can fix it. They don't want that vulnerability. (Maybe Microsoft is not the right one to pick on, but any of commercially available capability.) We have been trying to work with industry to share that kind of information, not to panic their stockholders, not to panic their banking individuals, but so that those vulnerabilities could be quickly eliminated. That's been a tough one. We've met multiple times with the banking industry, the telecommunications industry, and the electric power industry. We go through these issues and say, "Could we have some kind of mechanism for alerting each other to these vulnerabilities and try to get everybody to participate in that?" There's still a fear factor. "If I let you know, will you leak it? If you leak it, there goes the assurance of my company and, therefore, my profit, and then I'm out of business. You're not necessarily in that mode."

**Oettinger:** These problems are solvable, but it may take years and years. Look at the history of the census, where the government does guarantee confidentiality. On the whole it's been pretty good about maintaining the secrecy of individual information, because of the value of the aggregates. That also applies to certain types of economic data handled by the Department of Commerce. However, if you look at the political history of each of these, first, it has taken years and years, with acts of Congress, et cetera, to build that trust, and occasional breaches happen. Then the trust has to be rebuilt, and in a number of instances new issues arise, as with the sampling issue in the case of the census. If you talk about the financial services industry revealing every time X hundred thousand or million dollars gets stolen, it would really have to have a great deal of trust in the government to share that information with them.

**Roby:** We were surprised in some of those discussions just how much they write off. It's a phenomenal number that would really upset a lot of folks, but from their perspective they would rather write it off than let anybody know it.

**Oettinger:** It's only money.

Feb. 15, 2001. See Road Map for National Security: Imperative for Change, The Phase III Report of the U.S. Commission on National Security/21st Century, [On-line]. URL: http://www.nssg.gov/PhaseIIIFR.pdf (Accessed Oct. 2, 2001.)

[15] The cabinet-level Office of Homeland Security, headed by former Pennsylvania governor Tom Ridge, was established by executive order on October 8, 2001.

**Roby:** Yes. “It’s only money, and I’ll get more. If I let everybody know in some way, I may not get more.”

**Oettinger:** The pilferage rate in supermarkets is huge, but think about the security that would be required to frisk everybody going into a supermarket. There would be no grocery business at all. Again, those are industries where it’s only money. Imagine them talking across the table to folks from the Defense Department where it’s lives. It’s very hard to have a coherent conversation about money and lives.

**Roby:** As Tony said, this is going to take some time. We recently created something called the National Infrastructure Protection Center [NIPC]. You may or may not be familiar with this. It’s been in place for two and a half years. It’s physically in the FBI. One of the reasons we did that was specifically not to have it in the Defense Department, because of what the Defense Department is. Also, the FBI does have the responsibility for looking domestically, and we do not. That’s the role they’ve been endowed with. However, the NIPC has not been able to accomplish as much as was envisioned, and a lot of that is due to the trust factor not being there.

**Oettinger:** You’re being charitable. It was also predicted that they were incompetent over there, and they fulfilled the prediction.

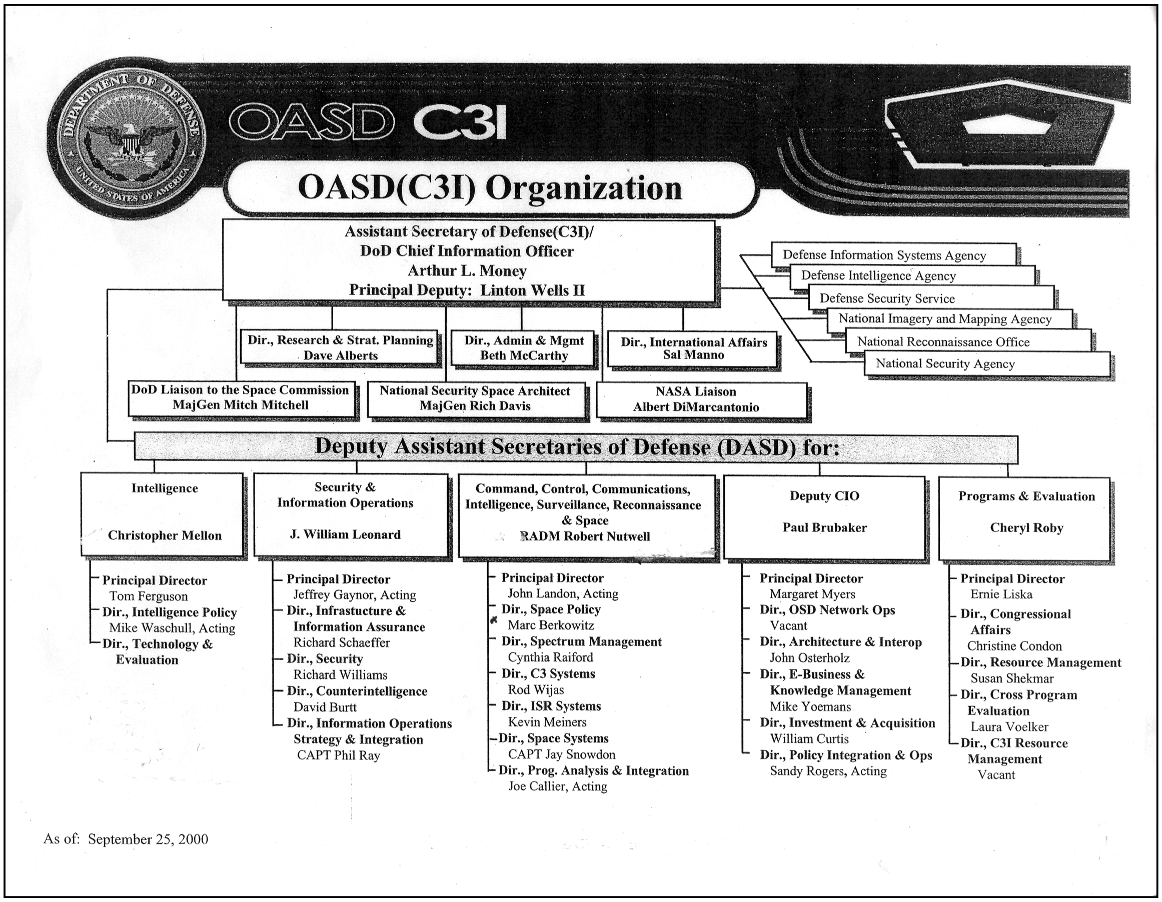
**Roby:** There are some difficulties being worked through. In fact, the deputy director of the NIPC, Admiral [James] Plehal, came from the Defense Department. He is a reservist who has been brought to active duty.

One of the other things I was going to come back to is information assurance and information assurance training. Another aspect we’re very concerned about is what we call “security in depth” or, to use a new term we’ve coined, “integrated protection.” What we’re talking about is looking across counterintelligence, infrastructure, and information assurance. How do we do those today? Are they as effective as they need to be? Can we do more?

First and foremost, what we discovered when we started examining this is that people weren’t trained. Some of the problems we were having were not the results of malice on the part of individuals. They just didn’t know what they needed to do. Going back to the example of software updates, they got the patches in and they just said, “When I get to it. No big deal, throw it on the side.” Systems administrators are very busy, and they are not, in most cases, trained in that business area. A lot of them were moved from other jobs into being systems administrators or LAN [local area network] administrators, because they had an interest or a competency in the business of computers. Somebody grabbed them and said, “Come on over, we’re going to do this.” We’ve learned that they don’t know what their responsibilities are, and now we’re getting them trained. We are spending significant amounts of money across all the services and defense agencies to ensure that they know what it really takes to do their jobs effectively. We’re making improvements in this business area as well

We also have introduced the subject of PKI—public key infrastructure, public key enabling—to go with the application software. That is one area in which investments have been made. We did it by taking the dollars from existing business accounts and saying: “This is such a priority that we [“we” being the secretary of defense, but the decision is based on advice that came from our office] direct you to invest more in PKI and do more to ensure that you are protecting the data that is flowing in the Defense Department.” That is getting a lot of press now, not only relative to the Defense Department. Many areas of business, as you just described, are looking at PKI as one of the solutions to the vulnerabilities that they all have.

I want to switch to just talking really quickly about the OASD C3I as an organization. I passed out an organization chart so you could see what we look like (**Figure 1**). I should have brought you one that shows how we sit within the overall Defense Department.



OASD C3I

OASD(C3I) Organization

Assistant Secretary of Defense(C3I)/
DoD Chief Information Officer
Arthur L. Money
Principal Deputy: Linton Wells II

Defense Information Systems Agency
Defense Intelligence Agency
Defense Security Service
National Imagery and Mapping Agency
National Reconnaissance Office
National Security Agency

Dir., Research & Strat. Planning
Dave Alberts

Dir., Admin & Mgmt
Beth McCarthy

Dir., International Affairs
Sal Manno

DoD Liaison to the Space Commission
MajGen Mitch Mitchell

National Security Space Architect
MajGen Rich Davis

NASA Liaison
Albert DiMarcantonio

Deputy Assistant Secretaries of Defense (DASD) for:

Intelligence
Christopher Mellon
- Principal Director
  Tom Ferguson
- Dir., Intelligence Policy
  Mike Waschull, Acting
- Dir., Technology & Evaluation

Security & Information Operations
J. William Leonard
- Principal Director
  Jeffrey Gaynor, Acting
- Dir., Infrastucture & Information Assurance
  Richard Schaeffer
- Dir., Security
  Richard Williams
- Dir., Counterintelligence
  David Burtt
- Dir., Information Operations Strategy & Integration
  CAPT Phil Ray

Command, Control, Communications, Intelligence, Surveillance, Reconnaissance & Space
RADM Robert Nutwell
- Principal Director
  John Landon, Acting
- Dir., Space Policy
  Marc Berkowitz
- Dir., Spectrum Management
  Cynthia Raiford
- Dir., C3 Systems
  Rod Wijas
- Dir., ISR Systems
  Kevin Meiners
- Dir., Space Systems
  CAPT Jay Snowdon
- Dir., Prog. Analysis & Integration
  Joe Callier, Acting

Deputy CIO
Paul Brubaker
- Principal Director
  Margaret Myers
- Dir., OSD Network Ops
  Vacant
- Dir., Architecture & Interop
  John Osterholz
- Dir., E-Business & Knowledge Management
  Mike Yoemans
- Dir., Investment & Acquisition
  William Curtis
- Dir., Policy Integration & Ops
  Sandy Rogers, Acting

Programs & Evaluation
Cheryl Roby
- Principal Director
  Ernie Liska
- Dir., Congressional Affairs
  Christine Condon
- Dir., Resource Management
  Susan Shekmar
- Dir., Cross Program Evaluation
  Laura Voelker
- Dir., C3I Resource Management
  Vacant

As of: September 25, 2000

**Figure 1**

The C3I organization is the only substantive organization within the Defense Department that is not at the under secretary level at this time. There are other ASDs—assistant secretaries of defense—but they're for legislative affairs and public affairs. What we're talking about here is an office with a business account that acts as a principal advisor for a business area. The comptroller who deals with the money is an under secretary; policy is an under secretary; acquisition, logistics, and technology is an under secretary; and personnel and readiness is an under secretary. We're the only ones who have equivalent responsibilities to the secretary—to report on command, control, communications and intelligence—but not in stature. As we were chatting about earlier, it's a very large portfolio. We're responsible to the secretary for looking at about a third of his overall budget. What our office does is tee up recommendations for the secretary. So do the under secretaries.

As our organization tries to point out, we have a deputy assistant secretary whose job it is to look at everything we talked about earlier: security, counterintelligence, information assurance, PKI, and information operations. We barely touched on that one at all, which relates to what we would do to ensure that we know what the enemy might do to our computer systems. We have computer network defense [CND], we have computer network exploitation, and we recently stood up something called computer network attack [CNA]. What would it take if we wanted to bring down one of our adversaries from a computer perspective? We're just barely scratching the surface of how that business area would be done. We have a deputy who is focused on policies and procedures, tactics, and techniques, all of that associated with the business areas I just quoted.

We have another deputy assistant secretary who has the job of looking at all the platforms, whether they fly in space or are airborne, surface, or subsurface platforms. That deputy assistant secretary is responsible for coming forward and saying, "These are the fixes you need to be making in that business area." That involves the communications, so a radio that could be used across all of the services that need radios to communicate comes out of that office.

That deputy assistant secretary is also responsible for spectrum. One of the most serious problems we had in the last several years is that some folks thought that auctioning spectrum to raise money would be good for the U.S. government as a means of getting dollars in our accounts. What they unfortunately hadn't thought through is that you don't get it back. Spectrum is finite. In the military, it's imperative to be able to communicate, and we communicate via the spectrum. We have to be able to talk without interruption, without delay, and we use the spectrum to pass information.

We managed in time to stop the sale of some spectrum where we already had platforms that were communicating using that part of the spectrum. As we speak, we are in the throes of possibly selling off even more spectrum, and that's going to cause us some serious concerns, because if we sell it we will have to vacate the spectrum. That means we couldn't use it any more for our military communications. Then where do we go? How do we change the equipment that uses that spectrum? It is very costly, and where would the money come from? How would we ensure all that? This office is responsible for teeing up this very serious problem to the secretary, getting his attention, and then getting the president's attention. The good news is that we're getting our arms around it, so we are slowing down the sales.[16]

**Oettinger:** The bad news is that, even assuming that everything that Cheryl has just described is successful, we ain't home free yet. Let's put it another way: It's worse than that, because although the government has made some money on it, the other policy objective was to make the spectrum available to a multiplicity of voices and promote competition, et cetera. It has resulted, actually, in the concentration of bidding among the largest organizations, and even they have bid so high that many of them have gone broke on the bidding and have no money left to do anything with the spectrum. Of course, in its own weird way, that may be the reason why you may be able to stop it and reacquire some of the spectrum. It's an example of unintended consequences of a policy that was narrowly regarded as being marvelous and economically very efficient in terms of selling at an auction, but there are sixteen other variables, of which Cheryl has hinted at some and I've added a couple of others, and there must be God knows how many more. It would be a

[16] See Harry D. Raduege, Jr., "DISA and NCS," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, September 2001), [On-line]. URL: http:www.pirp.harvard.edu/pubs.html

wonderful case study for some of you looking from here at an umbrella issue: the spectrum auction and how it screwed up the DOD and the whole industry in the name of a narrow conception of efficiency.

**Roby:** That would be marvelous. There would be a lot of interest in seeing that product pulled together.

**Oettinger:** As you said, society is very complicated, because once this goes up to the president, the president will say, “Oh my God, I’ve got to talk to the chairman of the FCC [Federal Communications Commission] (of course, he’s Colin Powell’s son), but then there are four other people on the FCC.” Before you know it, there are three years’ worth of hearings and who knows what will happen. So, as a Kennedy School-scale problem, this innocent-sounding thing is of an enormous magnitude.

**Student:** I’m trying to figure out from what I can read on the organization chart [Fig. 1] what’s going on between what Chris Mellon and the intel people are doing versus what’s going on in the middle under Admiral Nutwell. I see the platforms in his shop, but I also see space policy. What’s happened recently?

**Roby:** I would call that one of the oddities. What I was just describing in terms of the platform is what Admiral Nutwell does in the C4ISR [command, control, communications, computers, intelligence, surveillance, and reconnaissance] box. He’s responsible for development, acquisition, operations, and maintenance of platforms, as well as interoperability among platforms. In addition, an agreement was made that space policy, under Marc Berkowitz, would be retained in Admiral Nutwell’s shop. With the advent of the Space Commission and the new activities going on, my crystal ball would say that would not be sustained in a future structure.

What the policy activities for intelligence have focused on, what Chris Mellon works on right now, are things like personnel, training, and recruiting for intelligence, looking at the future environment in the twenty-first century. He would be the one who would go to what we call NIEs, national intelligence estimates, and say, “The threats of 2015 are asymmetric, and here’s what they are.” He’s looking at the long-range and also at some of the near-term policies.

Space is not just intelligence. Space is weather; space is navigation. The GPS [Global Positioning System] is one of the biggest elements of what we have in space, and you would not have put that under an intelligence office. No one would have expected the intelligence office to make decisions on GPS. Remote sensing blurred that, I’ve got to tell you. In the old days, remote sensing, or anything having to do with that, would quickly have been seen as intelligence, because that’s how you were using it. Now folks are saying that remote sensing can go beyond that. You’re looking at other aspects of how you would use remote sensing that do not necessarily have a direct correlation to just the intelligence aspects. Battlefield management is not intelligence. In the Air Force, at least, that is not an intelligence characterization. That’s just how they do battle management.

**Oettinger:** Hold on. I smell turf.

**Roby:** Yes, I’ve had that. That’s why Joint STARS [Surveillance Target Attack Radar System] is no longer a TIARA [Tactical Intelligence and Related Activities] program. For those of you who are not aware of TIARA, there’s an apparatus by which we look at U.S. intelligence. U.S. intelligence right now is jointly managed by the DOD and the DCI. Some of that money goes totally to the DCI, and he decides how much is going to go to the DIA, NIMA, NRO, and NSA [National Security Agency]. Then he has State, Treasury, and the CIA. He has to balance all his dollars and then the DCI and secretary of defense discuss the budget and agree on the right way to go.

Within the DOD, though, we manage another amount of money that's for joint programs. Mostly we use the joint account for airborne reconnaissance, but there's also some counterdrug money and counterintelligence money, because those are very joint. There's some money for doing research and development on cryptology that everybody would use. That's very joint.

The last one is TIARA, which allows the services to have the money within their accounts. Nobody else takes that money and manages it until the services are done with an activity, or at least until after they've proposed what they want to do. They are allowed to make tradeoffs with that money, whether they want to buy weapons platforms, or intelligence platforms, or more soldiers to do the cooking or the maintenance or actually be on the field, or intelligence soldiers, sailors, airmen, or marines. When they finalize that tradeoff the OSD has a chance to look at that and say, "That makes reasonable sense" or "No, I think you're putting too much emphasis on buying fighters and not enough emphasis on buying the intelligence that's going to make that fighter an effective platform. We're going to tell you how to reorient that money."

The biggest problem we've been having with the services is getting them to recognize the merits of joint programs. They take away from the services what would be unilateral decisions they could make about weapons platforms that they could have in their own organic service. On the other side, when you're going to go to a fight and you're at a joint task force [JTF], you want to have those kinds of interoperabilities. You want that jointness to be there. That was the premise behind why we take the money, give it to an executive agent, and ask the executive agent to do the best job it possibly can, within the dollars, for bringing that joint capability forward.

One for which I don't think we should get a gold star is UAVs, unmanned aerial vehicles. That was not one of our finest hours. We have a lot of problems. Maybe we've worked through some of those problems now, although I believe the jury is out at this point. We do have UAVs in each of the services, but we also are looking forward to a UAV that is more joint by nature. It's something we call the Global Hawk. Our biggest difficulty with the Global Hawk at this point is that it's an unmanned vehicle that competes somewhat with manned vehicles for resources. When you're giving it to an Air Force to manage there's some tendency for the Air Force to look more favorably upon manned vehicles than they do on unmanned vehicles. I don't know, there's something about them.

Where I was headed with that one is that there is a job to be performed that is more related to setting policy for intelligence. Chris Mellon's folks go to interagency meetings with the intelligence community that the DCI chairs. His focus is on bringing the intelligence community together. Admiral Nutwell's focus is on making the apparatus of intelligence platforms fit well, integrate well, into other DOD capabilities. One is more systems capabilities, the other's more policy.

**Student:** You had mentioned CNA very quickly. I understand it wasn't even an officially acknowledged phrase just a few years ago. Now that it's sort of come out of the closet and has been institutionalized as an organization, is that a reflection that we're no longer afraid of the repercussions of the term CNA? We were always thinking about countermeasures, counter-countermeasures, et cetera. If not, does the DOD have some transparency issues?

**Roby:** It's very complex at this point, but, yes, I would say that we are making progress. When we first started that business area, we actually called it information warfare, and as we started to wrestle with what it meant and how we were going to put it into the context of an approach to warfighting we were very leery. Once we declared information warfare to be one of the tenets of the business of the Defense Department, how would folks react? As you just said, how would our adversaries react? Would they then begin to build up an information warfare counterproposal or to counterattack in some way?

We wrestled with that for a long time. We actually changed the terminology and began calling it "information operations." We felt that term took it out of the realm of just using information in the weapon sense, and we gave ourselves the opportunity to really focus, early on, on what we thought was most important: defensive information operations. That means: are we watching? We don't want an electronic Pearl Harbor. How do we keep ourselves from ending up in that situation?

We put a lot of consideration, energy, thought, and infrastructure in place for this CND. You're right. In October 2000 we announced that not only did we have a JTF for CND, we also have a JTF for CNA. We stood up the JTF-CND two years ago in DISA, the Defense Information Systems Agency, formerly the Defense Communications Agency. We later realized it would be better to put it under a CINC [commander in chief of a unified or specified command] rather than a defense agency, so the JTF-CND was shifted to SPACECOM [U.S. Space Command]. We thought it would be the best place, with a vantage point looking across everything that we do. We then decided in to add CNA to the portfolio. We realized that it was time to accept and admit that there was a need for us to be prepared and to have CNA in our kit bag.

When the defense strategy comes out, it will have to be clear that this administration buys into the premise of information operations, both offensive and defensive, offensive being CNA, defensive being CND. I'm not sure that this administration has finished deliberations on what they're going to put in the national security strategy or the defense strategy with respect to CNA. In the Clinton administration we had made the conscious decision that we could go ahead and declare it, have tools available, and let the adversary know, "If you cross this line, we are capable of hurting you, and we will if you do." I'm paraphrasing it, but basically that was the language. I just don't know whether the Bush administration has that same commitment.

**Oettinger:** There are a couple of footnotes to note for the record. Going back a moment to the history of this whole question of how the alphabet soup got into the ASD C3I, there is a seminar presentation by Ruth Davis on the early history that we ought to cite here,[17] and then a more recent contribution by one of the budget people regarding the budget.[18] With regard to the

[17] Ruth M. Davis, "Putting C3I Development in a Strategic and Operational Context," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1988* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-89-3, March 1989), 161–174, [On-line]. URL: http:www.pirp.harvard.edu/pubs.html

[18] Thomas P. Quinn, "Acquiring C3 Systems for the Department of Defense: Process and Problems," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1994* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-95-3, January 1995), 1–28, [On-line]. URL: http://www.pirp.harvard.edu/pubs.html

question of attack, defense, and so on, two years ago Kawika Daguio, who was the American Bankers Association representative on the Critical Infrastructure Commission, gave a presentation here on some of the pros and cons of defense and attack in the financial services sector.[19]

I raise this, because I think it's important not only to look at what is liable to be attacked but also to ask questions about what is not likely to be attacked. One of the reasons why the financial services people think that attack is less likely, other than by the usual robbers, is that it is very difficult to tell whom you are robbing. If you attack any number of banks in, let's say, Europe or Asia, you are likely to attack U.S. property. Conversely, even if you are Osama bin Laden and attack a U.S. bank, maybe it's your own dollars that you are attacking. Therefore, if you follow some kind of rational actor view, it is in everybody's best interest to leave the frigging bank accounts alone, because the money you may be screwing up may be your own. I'm not suggesting that's the correct answer. I'm simply saying that these questions of what is a target, what is vulnerable, and what are the intentions as well as the capabilities, constitute an extraordinarily difficult intelligence problem. I give you this one about finance, because it's one of the clearest ones. Whether it's in anybody's interest to touch a hair on the head of that system is a very reasonable question to ask.

**Roby:** Yes. The use, in the past, of the term "collateral damage" takes on a very significant difference when we're talking about CNA, because you have no clue what you could be into when you push that button or send that zero instead of that one. It does give you pause, and the administration would have to decide if this is really something we're sufficiently serious about to want to put it into motion and do something. What we've agreed is that we've got to learn more about it, understand it better, and really analyze it if we ever intend to do something, so we've agreed to do CNA as a business area, with SPACECOM in charge of both CNA and CND.

**Student:** We can create scenarios and think about possible computer attacks and knock-downs. What about the attacks that people on the street, like myself, cannot even imagine happening? Do you in the DOD have a component that does research on what the possible attacks might be ten years down the road? Would it be similar to private industry—for example, to the Xerox research centers that look at what is twenty years down the road and what technologies are going to be prevalent?

**Roby:** We use the intelligence community to tell us what they think the threats are going to be—global threats and threats to the homeland. We do analysis to try to build maximum information, which we then publish to our seniors. We say, "This is the trend that we're seeing, therefore these are the threats and the challenges we're going to have." Rick Raftery, who is here with me today, has looked at the potential threats in urban areas. What would those threats be? How would we deal with them? We try to think through those. I'm not aware of a specific center that does nothing but that.

As I said, there are groups of people who are always looking at what's twenty years out and doing assessments that bring our attention to those issues. They will ask questions like, What happens to the DOD if the blood supply is tainted? One study they did recently was, what would

[19] Kawika Daguio, "Protecting the Financial and Payment System by Dispelling Myths," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1999* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-00-2, June 2000), [On-line]. URL: http://www.pirp.harvard.edu/pubs.html

happen if somebody went to the opera, let's say in Boston, and an adversary brought a strain of flu there and did an aerial dispersal? What would you do? How would you know it? What would you do about it? How devastating would it be? They try those as part of what we call exercises or demonstrations or experiments or things like that so that we think along those lines, but I don't know of any group that does only that.

**Student:** So they think more along the lines of conventional wisdom. In terms of technology around thirty years ago, people probably wouldn't have thought about the [computer] mouse.

**Roby:** You're triggering me. There are groups that support the Defense Department. They're not in the Defense Department. We hire groups of people who are thinking great and really expansive thoughts, and a number of those produce materials for us.

**Oettinger:** On April 5, Captain O'Neill will be here from the Highlands Forum. Ask the question again of Dick O'Neill.

**Roby:** That's exactly the one I was going to suggest. We hired that group. Actually, OASD C3I as an organization chartered the first meetings of the Highlands Forum.[20]

**Oettinger:** Dick O'Neill was deputy for strategy and policy in the OASD C3I at the time.

**Roby:** Yes, but even before he was a participant, a general officer in the Air Force[21] came on board as our principal deputy, and he had the first germs of the idea that you need to have somebody who's looking at nanotechnologies. What does that mean, and how would that evolve? They're now thinking about things that go beyond conventional wisdom, as you just described it, and looking at ways of expanding our expectations and then asking, "If we're going to get there, what are the things we'll need to be doing in the interim?" There are several of those kinds of groups.

**Student:** Can these groups also sell the information to China, for instance?

**Roby:** Some can, some can't. Sometimes when we use DOD money one of the first things we do is have them sign nondisclosure agreements that say they can give this to any government that we approve, or that they can give it only to the U.S. government. "We're giving you this money to do this analysis and we restrict whom you can show it to." Most of the time I would suggest that's what we do up front.

**Student:** That brings up one of my favorite questions. You've been talking about UAVs, about public assets, intelligence assets, and national technical means that are in the public sector. What do you do when private citizens or people in other governments start getting public sector information, such as overhead views of naval bases or of foreign deployments? What does OASD C3I do about that? Or don't you do anything?

**Roby:** Let me pull it two different ways. There is no restriction at this point on dissemination of aerial imagery—meaning aerial done either by air breathers or by satellites. However, if it's a U.S. company, we have restrictions in the licensing agreements that in a wartime situation they

[20] 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); [forthcoming].

[21] Major General Frank B. (Barry) Horton (1940–97).

must limit distribution (we call it shutter control) for a minimum of twenty-four hours. We can actually make it longer than that depending on the crisis situation. An adversary would not be able to get an image of a naval base or of a beachhead where we were going to land some forces within a window of opportunity. We would restrict their ability to get it. In peacetime, there is nothing I know of that does anything to limit the collection, distribution, or dissemination of overhead—aerial or satellite—imagery.

**Oettinger:** May I again make a comment on that? Think about the balancing acts there. The availability of overhead imagery was one of the great stabilizing factors throughout the whole cold war period, so this can be regarded as an asset as well as a liability. Again, it's not an easy decision which way you go.

**Student:** Isn't that sort of the basis behind the Open Skies treaty?

**Roby:** That's exactly right. The Eisenhower Open Skies proposal.[22]

**Student:** I'd be more worried about Osama bin Laden being able to go through an intermediary to get overheads of a naval base. One of the students in this class is working on terrorism and security for naval bases. If an adversary can get good, high-resolution overhead images of those, it could be a problem. Are we working on even peacetime regulations of that type of thing vis-à-vis terrorism or not?

**Roby:** I am not aware we are doing anything about that. For U.S. companies, we only deal with the issue when we do the licensing. For foreign companies, we have no restrictions at all. It's an open, free society and whether you're an adversary of the United States or not, you're allowed to purchase the images that are produced by these for-profit companies. There's nothing we can do to restrict those.

One of the good things that's happening so far is that the resolution isn't that good. That helps somewhat, but one day I may not be able to make that statement.

Like our adversaries, we try not to put things in the open so that they can see it. We would use denial and deception, or concealment. There are things about which we very much want to minimize their knowledge so that they can't exploit them as a vulnerability, but we can only go so far, especially if you're talking about a naval base.

**Student:** At the first meeting of the U.S.–Russian Environmental Task Force, which was partly sponsored by the NRO, one of the first things that happened was that the Russians said, "We want to show you our beautiful overhead pictures of the new NRO building," which had just been completed. Of course, they had the best imagery of the western hemisphere, and we had the best imagery of the eastern hemisphere.

**Roby:** I was just going over the C3I organization. We talked about the DASD for intelligence, and you asked what that office does. Its real focus for intelligence is making sure that knowledge is exchanged between the Defense Department and the DCI in every way we possibly can. It pulls together positions for the services and other elements of the Defense Department to take into a meeting in an interagency forum. The DASD for intelligence is at the table representing the secretary, the deputy secretary, and the services. We do have the services in some of the meetings

[22] The Open Skies Treaty established the regime for conduct of observation flights over the territory of other nations. The idea was originally proposed by President Eisenhower in 1955.

when we’re really talking about substance and production, but in general policy settings we don’t have them there. That’s why that office exists.

The DASD for intelligence, surveillance, and reconnaissance would go to a meeting where we’re talking about a future capability and say, “It needs to be *this* big, *this* wide, *this* small”; that kind of stuff. The DASD for intelligence wouldn’t normally be available for doing that.

**Student:** I was curious about the split. When the policy was put out, it seemed logical that the space policy folks would have been in the same group of people as the intel policy people.

**Roby:** I do think that’s going to come. Watch this space! Let’s see if we stand up an under secretary for space, intelligence, and information. Would you then have a space, an intelligence, and an information box underneath? Would you have assistant secretaries for each of those, or would you have it integrated in some way? Would you have an assistant secretary for space and intelligence? Based on the way you and I just talked about it, without a doubt, because why would you not want them to have one boss watching over, directing, and guiding the actions that need to happen? Then you could put information—things like communications, command, and control—under the chief information officer [CIO].

The CIO came about because Defense Secretary [William S.] Cohen, when he was a senator, created something we euphemistically called the Clinger–Cohen Act, because he and Senator Clinger were the two who put this together.[23] The CIO reflects an expectation that the information age needs an overseer whose job it is to watch, guide, direct, and ensure success in the mission areas of the Defense Department. The function was designated to our organization. So, another reason that the CIO exists is to improve the ability of the entire Defense Department in this area and then take part in a national forum where all the CIOs from all the cabinet departments meet and try to design a federal approach to information.

We have now started to expand this internationally, so that we’re talking to the Japanese, the Brits, and the Australians about this. They’ve actually superseded us somewhat, because they’re talking about a “chief knowledge officer” instead of a chief information officer. We may make that switch as well here in the United States. Basically, what that responsibility leads to is standardization, or the ability to come up with policies and guidance where you’re looking at capital planning and replacement. You’ve got to invest for the future. You’ve got to invest properly in the infrastructure. Someone should be helping to make you smart. We’ve created and coined “portfolio management” as the way we need to be going. That’s another of our tenets.

Those are the major components of the C3I organization. We’re a bunch of bureaucrats. We come to work every day, and we try to help, advise, and guide the secretary on the decisions he needs to make. We do think that the most overarching thing we can do for him is to ensure that his data are prepared properly, that the data are secure when they are sent, that we can authenticate who’s getting the data, that there’s nothing bad happening as data are flowing, and that, finally, the data are in the right format when they get to the end user so the information can be used by an effective manager. Every one of the five boxes [the deputy assistant secretaries] is ultimately trying to do that every day.

In addition, we oversee the entire intelligence apparatus. The DIA, the NIMA, the NSA, and the NRO all report to Arthur Money, the ASD C3I, for guidance, advice, and direction. That’s

[23] The intent of the Clinger–Cohen Act of 1996, previously called the Information Technology Management Reform Act, is to improve government performance through the effective application of IT.

done on a cooperative basis. It's not an edict that comes down. Those folks meet every month with Mr. Money. Once a week they have their representatives come to a meeting with Mr. Money. There's a lot of information exchange to try to keep surprises from happening and to keep people abreast of what's going on.

In addition, Mr. Money is responsible for DISA. We talked about them before. They do the communications. He's also responsible for security services and clearances.

**Oettinger:** You'll have, by the way, an opportunity to see three of those gentlemen. Hayden of the NSA, Raduege of the DISA, and Wilson of the DIA will be here, so you'll have an opportunity to hear their side of their side of that story.[24]

**Roby:** Ask them how well that it works. I think it's an imperative, though. Those agencies have to have someone whom they can call upon to be their interface to the secretary and the deputy secretary. It's rare to get a lot of audiences, because those folks are busy. Mr. Money, or whoever is in the position, is in a meeting with the secretary or the deputy secretary every day, so you want to have that kind of a relationship. The question is, how authoritative, how directive, how micromanaging do you want that responsibility to be? There are often items that cause concern. We work through them and we bring back, we hope, a cooperative relationship between the six agencies and Mr. Money.

Speaking of Mr. Money, he has been in the position of ASD C3I for almost three years. He will be leaving us by the end of April and moving on to some other position.[25] We are unsure exactly what the secretary is going to do. We're hoping the timing is going to work out and that as Mr. Money leaves he will say, "We are going to make this an under secretary and here's whom we want," or "It was an interesting suggestion that the Space Commission had and we may think about it further on," and leave it as an ASD C3I, as we are today, but still tell us who the new person is going to be. In the interim, we have a principal deputy. Linton Wells will be acting for the C3I organization until we finalize that.

**Oettinger:** On that note, I hate to bring this to a close because it's going so marvelously, but the next folks will be invading shortly and it will be time to clean up. So, I thank you for a splendid discussion.

**Roby:** You're very welcome.

**Oettinger:** Here's a small token of our great appreciation.

**Roby:** Thank you. That's terrific. I appreciate it. Thank you all very much. To anybody who has any other questions, I have an e-mail address. I brought some cards, and if anybody wants to take one of those I'm delighted. The address is on the Internet. It's unclassified, so be careful if you want to send something that has to do with security aspects.

[24] See, in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3), Michael V. Hayden, "The Roles and Responsibilities of the National Security Agency"; [forthcoming], Harry D. Raduege, Jr., "DISA and NCS" (September 2001), and Thomas R. Wilson, "Asymmetric Approaches to Joint Vision 2020" (November 2001), [On-line]. URL: http:www.pirp.harvard.edu/pubs.html

[25] John Stenbit succeeded Mr. Money as the ASD C3I on August 7, 2001.

## Acronyms

| | |
|---|---|
| ASD | assistant secretary of defense |
| C3I | command, control, communications, and intelligence |
| C4ISR | command, control, communications, computers, intelligence, surveillance, and reconnaissance |
| CIA | Central Intelligence Agency |
| CIO | chief information officer |
| CNA | computer network attack |
| CND | computer network defense |
| DASD | deputy assistant secretary of defense |
| DCI | Director of Central Intelligence |
| DIA | Defense Intelligence Agency |
| DOD | Department of Defense |
| FBI | Federal Bureau of Investigation |
| FCC | Federal Communications Commission |
| GDIP | General Defense Intelligence Program |
| GPS | Global Positioning System |
| I&S | intelligence and security |
| IT | information technology |
| JTF | joint task force |
| NIMA | National Imagery and Mapping Agency |
| NIPC | National Infrastructure Protection Center |
| NMD | national missile defense |
| NRO | National Reconnaissance Office |
| NSA | National Security Agency |
| NSC | National Security Council |
| NTIC | Naval Technical Intelligence Center |
| OASD | Office of the Assistant Secretary of Defense |
| OSD | Office of the Secretary of Defense |
| PKI | public key infrastructure |
| SPACECOM | U.S. Space Command |
| TIARA | Tactical Intelligence and Related Activities |

| | |
|---|---|
| UAV | unmanned aerial vehicle |
| WMD | weapons of mass destruction |

INCSEMINAR2001

ISBN 1-879716-76-3