INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

C^3I In Transition
Albert R. Lubarsky

Guest Presentations, Spring 1992
Frank B. Horton; Roscoe M. Cougill; James J. Hearn; John M. McConnel; Richard L. Haver; Albert R. Lubarsky; Richard J. Kerr; Richard C. Macke

August 1994

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-16-x **I-94-4**

C³I in Transition

Albert R. Lubarsky

Mr. Lubarsky is the Department of Defense Director, C³I for Counternarcotics, a position he has held since May 1990. Previously, he served as the Deputy Assistant Secretary of Defense for C³, Office of the Under Secretary of Defense for Acquisition. His earlier positions for the Office of the Secretary for Defense (OSD) include Director, Mission Assessment and Evaluation and senior staff assistant in the Office of the Under Secretary of Defense for Research and Engineering. Before going to the OSD, he served as a senior member of the technical staff, Office of the Chief of Naval Operations, and engineer and engineering manager with the Department of the Air Force. Mr. Lubarsky is a senior member of the Institute of Electrical and Electronics Engineers and is active in its Communications Society and on the executive board for MILCOM.

Oettinger: It's an especially great pleasure to introduce Al Lubarsky. As you will have seen from his biography, he has seen them all, including something that I did not grasp earlier. Clearly, as a civilian, he had worked with both the Air Force and the Navy and then, of course, currently in the Office of the Secretary of Defense (OSD) in his capping role, so I said, "Well, what about the Army?" and it turns out that's where he did his military service. So, if ever there was a tri-service-cum-purple person with experience going way back, that's Al, including these days being so modern and contemporary as to be doing C³I for counternarcotics. So, he will tell us something about his life and times — an unusual combination of both contemporariness and historical perspective. Al, it's all yours.

Lubarsky: Thank you for the wonderful introduction. I had a few pages of things I wanted to get through. I hope that, in a small group like this, we can keep it very informal, so feel free to raise whatever observations or questions you may have as we go through this, and if it looks like I'm not going to get to the end of four or five pages, I'll try to slow down or whatever is appropriate. I'm certainly not going to make this a formal briefing.

The first thing I want to do, if it would be acceptable, is make a few comments on some of the issues that are raised in Tom Coakley's edited transcripts of the previous speakers,* only because I can't resist. One of the comments I'd like to bring up first would be some of the — it would seem to me — superfluous sorts of arguments that have been raised about whether command and control is a process, an esoteric thing, or as a practical matter, whether the real practitioners of command and control are theoreticians or operators. It goes with the gist of trying to define C³I from my perspective.

Analogies don't always get to the point, but I look at C³ systems like any reasonably complex system, perhaps an automobile. There are people who design automobiles, who know the rules of mechanical engineering and lately also electronic engineering in order to put cars together. We have the casual driver, who probably is not interested at all in how the car operates, only in the fact that it turns right and left and gets people where they want to go on Sunday (or whatever day they choose). And, of course, somewhere in between, there are people who combine some talents of each, perhaps race car drivers or test drivers or something of that nature. The same analogy goes for aircraft. A pilot, perhaps, has a little more skill than a Sunday driver, but may be ill equipped to do aerodynamic design on aircraft.

*Thomas P. Coakley, *C³I: Issues of Command and Control*, Washington, DC, National Defense University Press, 1991.

I think when we get to C^3 systems, we have a similar analogy for one reason. We have operators who, as commanders and as members of a commander's staff, don't really care how the system works. They picture themselves as tacticians, or strategists, or leaders of people. But, whatever their viewpoint, they are faced with putting up with a command and control system and infrastructure that is perhaps not foreign to them, but one with which they are not intimately familiar. Of course, we have the technologists who designed this system: like all designers, some know about tactics and strategy and some don't; however they do, obviously, know the rules of physics and engineering that are required to make such things hum. Then we have the modern model of a commander who is the equivalent of the race driver or the test pilot, who has enough technical background that he (he or she, in the future, one would hope) can appreciate what systems have been provided to accomplish the task of commanding troops in battle and controlling weapons; and also has enough background to practice the military arts. That may be obvious when you think about it the second time; however, I thought there was a lot of verbiage being wasted by some of the speakers who argued that "wireheads" and "propeller heads" and people of this sort are not "real C^3 people:" only people in the field are the "commanders and controllers." From that I will go ahead and try to define what I was going to talk about.

First, if you were to look at C^3I systems in the field, or C^3I in general, what do you see? What is the tangible proof that such a thing exists, and what do we buy with our C^3I budget? (which has been considerable). I want to go through what one buys in just a little detail. It may be obvious to some of you, and, if so, I can keep it short.

As Capt. Frank Snyder (USN Ret.) brought up at lunch, telecommunications was obviously the first thing included in the C^3 budget. From the historical perspective, when we started building C^3 systems, the primary importance was given to strategic communications for connectivity from the National Command Authority down to the echelons that provide weapons release authority. Historically, air defense systems have always been closely associated with C^3 since various air defense nodes must be tied together with telecommunications. As an illustration, SAGE (Semi-Automated Ground Environment) was the first U.S. automated air defense system designed in the 1950s by Bell Labs and others. When it was fully operational in the early 1960s, AT&T had a monopoly on long distance phone service, and the phone bill to tie the nodes together was about $1 million a day in 1960 dollars, which would be a lot of money in today's world. So communications cost and the equipment used to communicate have always been considered part of C^3.

Moving down the chain, tactical communications systems have been in the C^3 budget for quite some time. The long haul systems, such as the Defense Communications Systems, military communications satellites, COMSEC (communications security), and others are included. More recently, the C^3I budget has been expanded, at least from the Secretary of Defense's perspective, to include almost all DOD telecommunications, which encompasses the administrative type of phone service that is provided at bases, posts, camps, and other places where DOD does its business — telecommunications that tie together the business functions of an organization. So, whether you look at C^3I in the budget, or kick it in the field, the category now pretty much includes all telecommunications.

What we used to call ADP — automated data processing, or computers — is a little different. The so-called embedded computers, the computers that actually make weapons systems work and may be embedded in missile launchers or things of that nature, have typically not been in the C^3I budget and are not considered C^3I in the Department of Defense. The C^3I function for weapons systems and platforms is usually considered as being above (i.e., at a higher level than) the weapons system itself, allowing people to utilize weapons systems and to plan for their use. It's sort of arbitrary.

Oettinger: The arbitrariness, though, is not altogether capricious. My recollection of the history is that when Congressman Jack Brooks got his bill passed, which put a lot of rather difficult conditions on the acquisition of computer systems, an awful lot of what used to be computer systems then became embedded systems in weapons and disappeared from under the Brooks bill.

Lubarsky: That was true for a while. Of course, we had the Warner amendment to the Brooks bill, which specifically allowed critical C^3I — whatever that is, since it assumes there is some noncritical C^3I — to be included. Those of us who are practitioners don't think any of it is noncritical, obviously.

Oettinger: I made the comment simply to get on the record that nontechnical or political factors often have a way of making very intelligible something that on the surface might look arbitrary.

Lubarsky: That's true. In general, a lot of the large mainframes, which are used in command and control systems like WWMCCS (Worldwide Military Command and Control System), and others you may have heard of, have been in the C³I budget from the start. The computers that the CINCs (commanders in chief) use for their command centers, typically air defense center computers above the weapons level, have been included in C³ budgets as have those at submarine warfare centers ashore in the case of the Navy, and ruggedized MIL SPEC kinds of computers that are intended for tactical use in Army or Marine Corps command center vehicles, tents and shelters. That's traditionally what's been in the C³I budget.

Now, with the new breakout, and with corporate information management (CIM) and information resource management (IRM) becoming buzzwords in DOD, it turns out that the C³I budget is picking up more and more responsibility for ADP systems across the board, whether they're for business use or not. That's again sort of arbitrary, but as we look at more modern computer architectures, it becomes more obvious that if people are keeping track of logistics and aircraft — the equivalent of airline reservation systems for the military — with the technology at hand today and with the concepts of organizational downsizing, the information contained in those systems may be very useful for C³I purposes. Maintaining it separately in a non-interconnected way doesn't make a lot of sense, even though in past generations of hardware it may have been just as easy to keep it separate. Now it appears that the move toward integration is going on. We keep personnel manpower records in nine or ten different echelons. The medical people, the payroll people, the personnel people who are in charge of training, the manpower people who are attempting to move people to the active units, all keep their own systems. It's obvious that there has to be some interplay among all those activities. It would be nice if one entry, for instance, that stated that a front line unit needed a new tank driver could wend its way through all these systems, so that the pipeline would start training new tank drivers, medical records would be pulled up because the reason we need a new tank driver is because the last one was hurt or wounded, and so on. With the technology and the networks we're speaking of today, it appears that more and more information that was always on the periphery of the C³I processes is now more easily accessible and is becoming more involved in the C³ process, so it's pretty hard to say where the C³I use of ADP starts and finishes. The old traditional lines are fading, and more and more of these systems are being put into the C³I budget.

Of course, C³I includes the command centers themselves. It's pretty obvious that a command center can be anything from the basement of the Pentagon, out to the command centers for the Commanders-in-Chief and their subordinate units, down to tactical command centers in the back of an Army-type vehicle, command centers aboard ships to a certain extent, the new airborne command posts (707s and 747s). So those things are typically included in the C³ budget.

The really fuzzy areas is sensors. The C³I process requires some inputs for commanders and their staffs to make informed decisions. These inputs come from sensors, and the typical model, which I'm sure you've all been exposed to, is some iterative process where sensor input comes to a command center and then gets communicated out. It's a simplistic way of looking at things. For one reason or another, as Professor Oettinger pointed out, because of politics and the way things are funded, some sensor systems have traditionally been in the C³I budget and some not, and some with good reason and some otherwise. The AWACS (Airborne Warning and Control System) — the E-3 aircraft in OSD's parlance — has always been in the C³ budget. The Air Force, however, treats AWACS as another aircraft program and the money for AWACS tends to be in the aircraft procurement line. The E-2C — the Navy's equivalent airborne early warning aircraft — is the same way: in OSD and congressional parlance it has been a C³ platform; in the Navy it's not, it's part of the air warfare budget. So there's not even a complete match between the services. TACAMO (Take Charge and Move Out), which is the communications relay aircraft, has been one we've agreed on: the Navy's always kept that in the C³ budget, which has skewed the Navy C³ budget for years, because one large Boeing 707-type aircraft costs more than a lot of small radios, as you can imagine.

The other things that have been put in the C³ budget over the years are the navigation and timing systems — LORAN (location, ranging, and navigation), and NAVSTAR — global positioning system (GPS).

The big thing in the C³ budget, of course, has been manpower. It takes a lot of people to run those systems. At one time in the late 1980s there were more signalmen and communicators in Central

Europe than there were tank drivers. There were almost as many as infantrymen. So anyone who thinks that this is a transparent cost and only hardware is expensive doesn't have a good feel for field conditions.

One other thing just in passing. Sensors, jammers, and things of that nature for electronic warfare (EW) which is the active part of disrupting other people's C^3 systems, at various times are considered part of the C^3 budget and part of C^3 in management structure, and sometimes they're not. In 30 years I've been through several cycles. My theory is that when EW programs are in trouble, people want to get rid of them if they have the power to do so! It's about as good a rationale as any!

I'm going to give you a quick breakdown of what the C^3 resources have looked like from an OSD perspective in recent years. These are brand new charts; they were just delivered to the congressional hearing today, to the House Appropriations Committee, Chairman Murtha's subcommittee. They're reasonably close to being right. We've broken these down by the three basic C^3 mission areas. If we get involved in intelligence or in communications security devices, some of the numbers get classified, so we tend not to use those. Anybody who is really interested can find the total numbers and the C^3 numbers and can back one out of the other to make an educated guess, but we don't print them.

FY 1992 supposedly started on October 1 (figure 1); however, Congress passed the budget on December 5, and we didn't get the money through the system until about January 20, so we're just about starting to pay the bills for FY 1992. There is $18.4 billion, roughly, in the traditional C^3 end of the budget. It's divided more or less into thirds. Defense-wide C^3 is the long-haul communications, satellite circuits, leased communication systems, major command centers of the commanders-in-chief of the unified commands. Theater and tactical tends to be weighted towards Army units, which buy a lot of individual radios to keep everybody in communications. Strategic, of course, has been the big kicker over the years. It has started to come down, but that is the current figure.

Student: You talk about the Army wanting all the radios that came out of your budget. They came out of the Army's budget.

Lubarsky: Let me make that clear. OSD does not have a C^3 budget. The Congress budgets money directly to the military departments that are lead for a given system, or that have the procurement authority to buy it; the Joint Chiefs of Staff and the Office of the Secretary of Defense try by various means to influence the military departments to procure and operate C^3 systems for the common good of the C^3 mission of the Department of Defense. I guess that's a roundabout way of saying that we jawbone, and depending on who the personalities are among the military department heads and the Secretary, we do have some influence. We also write or approve specifications, put out standards, national and international, etc., but the actual money is in the military department budgets. Also during the budget preparation, OSD does play a role.

Getting back to the chart, the Army numbers are large since there are a lot more infantry squads than destroyers. A destroyer may require 12 or 15 radios while each infantry squad needs one or two. So the big multiplier in tactical C^3 tends to be the Army and Marine Corps.

Strategic C^3 tends to be heavily Air Force oriented because the Air Force, as you probably know, operates two thirds of the strategic triad — the missile force on land and the bomber force are both Air Force-funded. The Navy funds in strategic are for sea-based assets, such as submarines.

Defense-wide is sort of a mix. The C^3 budget has basically been constant. It's down a little bit, of course, because the defense budget is down. It hit a high when it was in the $21 billion to $22 billion range in 1986 and 1987. We're running at about $18 billion now. The 1992 figure is actually appropriated and authorized. FY 1993 is the budget request, which is currently being considered by the Congress; it is the "President's budget" and has been requested from the Congress.

The thing you asked about is shown next, a breakout by component (figure 2). Again, that tends to be roughly the same percentage over the years. The Air Force typically spends about half of the DOD C^3 budget, because the Air Force does man and operate and pay for two thirds of the strategic C^3 systems. There are also a lot of tactical sets in the Air Force: command and control for tactical aircraft, air defense and air traffic control types of things, especially in Europe, are in the Air Force budget. You see the Army and the Navy. The "other" tends to be the defense agencies, which typically manage a lot of programs but don't procure or operate much of their own. They also tend to pass on requirements to the military departments for funding.

The last breakout that I was going to use, and then get away from these pie charts, is what we do with the funding (figure 3). These numbers have changed

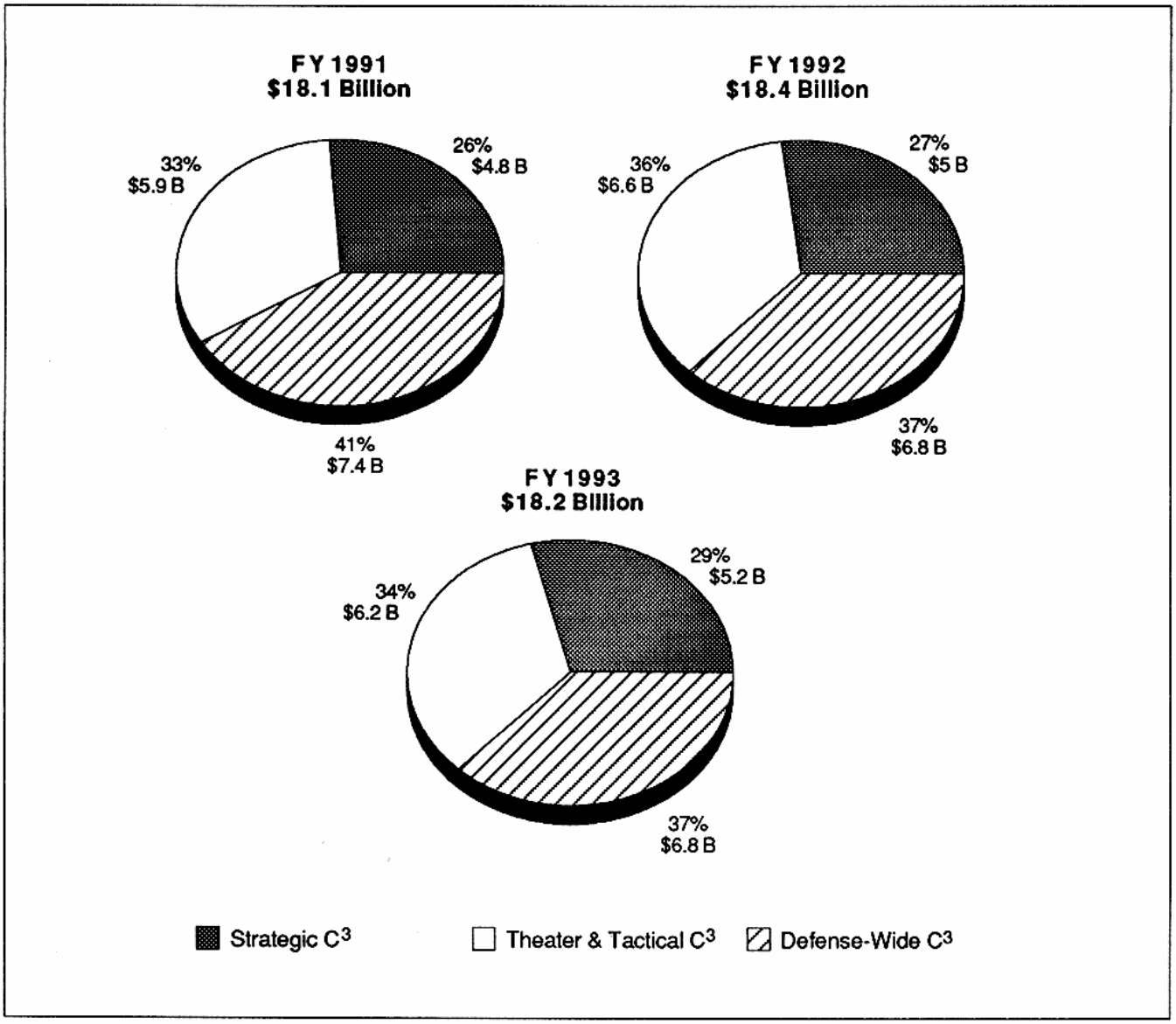

Figure 1
C³ Resources by Mission Area ($ in Billions)

dramatically over the years. RDT&E is research, development, testing, and evaluation — the resources needed to develop new C³I systems. Procurement is the actual buying of the hardware. O&M is the operational cost, other than military personnel. That's the civilian pay to run all these things, and the expendables, the minor items to keep things going — the fuel oil to run the generators, the paper to put in the computers, pieces of cable, printer ribbons, and the forests we need to cut down to make enough paper for all the 12 million messages we send each other every year. The military personnel (category) pays the direct salary costs of some of the people who are involved in running the C³I systems, but a lot of them are not paid out of the C³I budget; they're around for other reasons. For instance, the commander is obviously needed to command, and doesn't get paid out of the C³I budget. The mix is different in the various military departments. Typically, the C³I budget includes almost no one's salary on a ship; most shipboard operators are paid out of typical Navy personnel

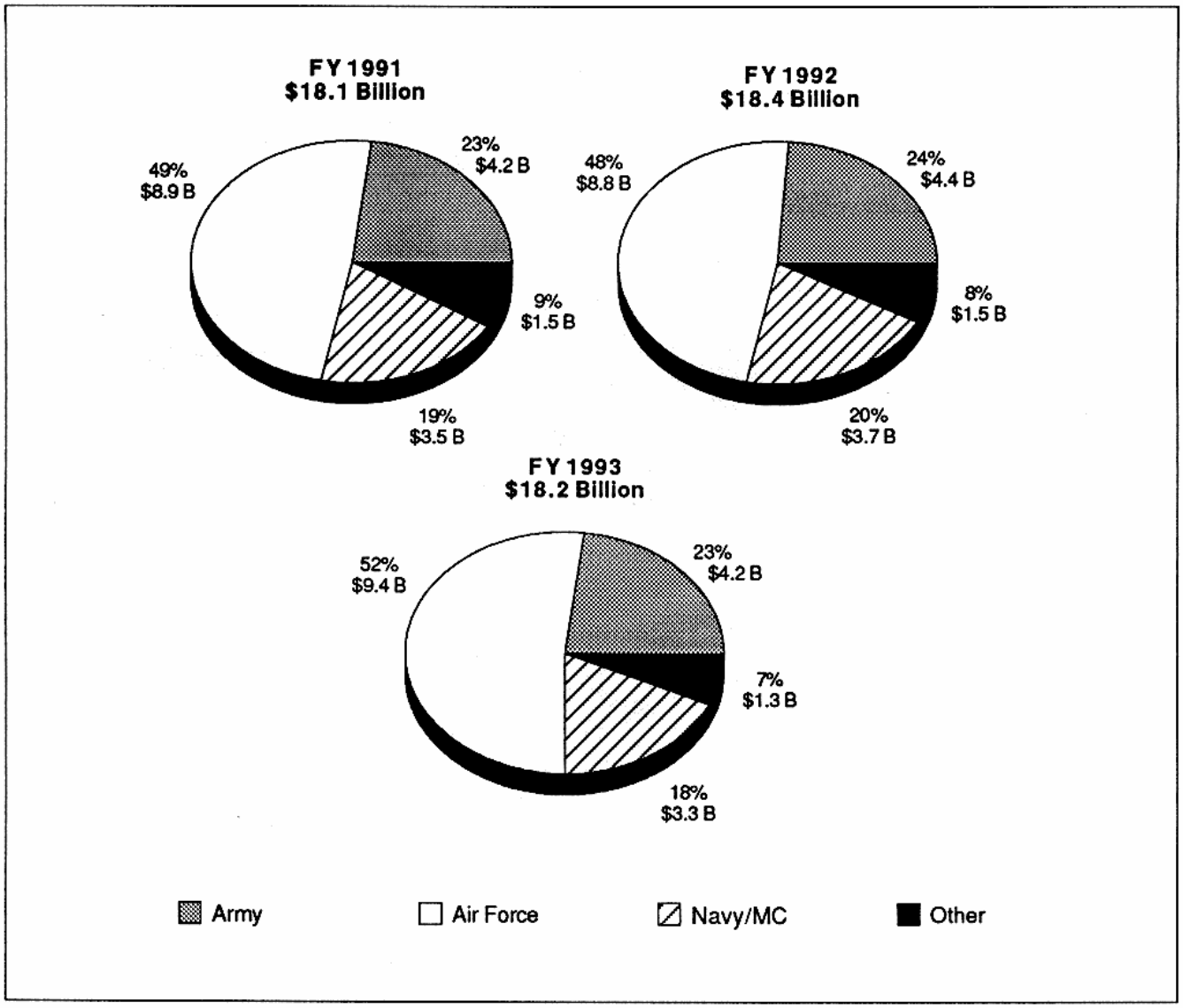

Figure 2
C³ Resources by DOD Component ($ in Billions)

costs, so none of the manpower items can be compared directly. I offer them more as an order of magnitude and as a breakout of how these things work, rather than as any exact numbers; taking them down to tenths of a billion, tells how exact they are.

With that, I was going to leave the budget discussion, but let me just say one thing about it. The traditional C³ functions I showed have varied between 4 and 7 percent of the total defense budget for the last 15 years or so. Now, these numbers shown are obviously over 4 percent, assuming the defense budget is going to be somewhere between $200 billion and $300 billion this year. A safe guess is closer to $300 billion; your educated guess on that might be better than mine. It's gone up and down during the years, and this year, because we have picked up the additional things mentioned in information resource management and other places, some of the numbers you might see in the open literature will be considerably higher; and a lot of the commercial ADP systems and other things of that nature may be "racked up" within the C³I budget, making comparisons more difficult.

The next thing to mention is what C³I does for DOD. I tried to explain in some detail what you see if you go out into the field and look for C³I systems

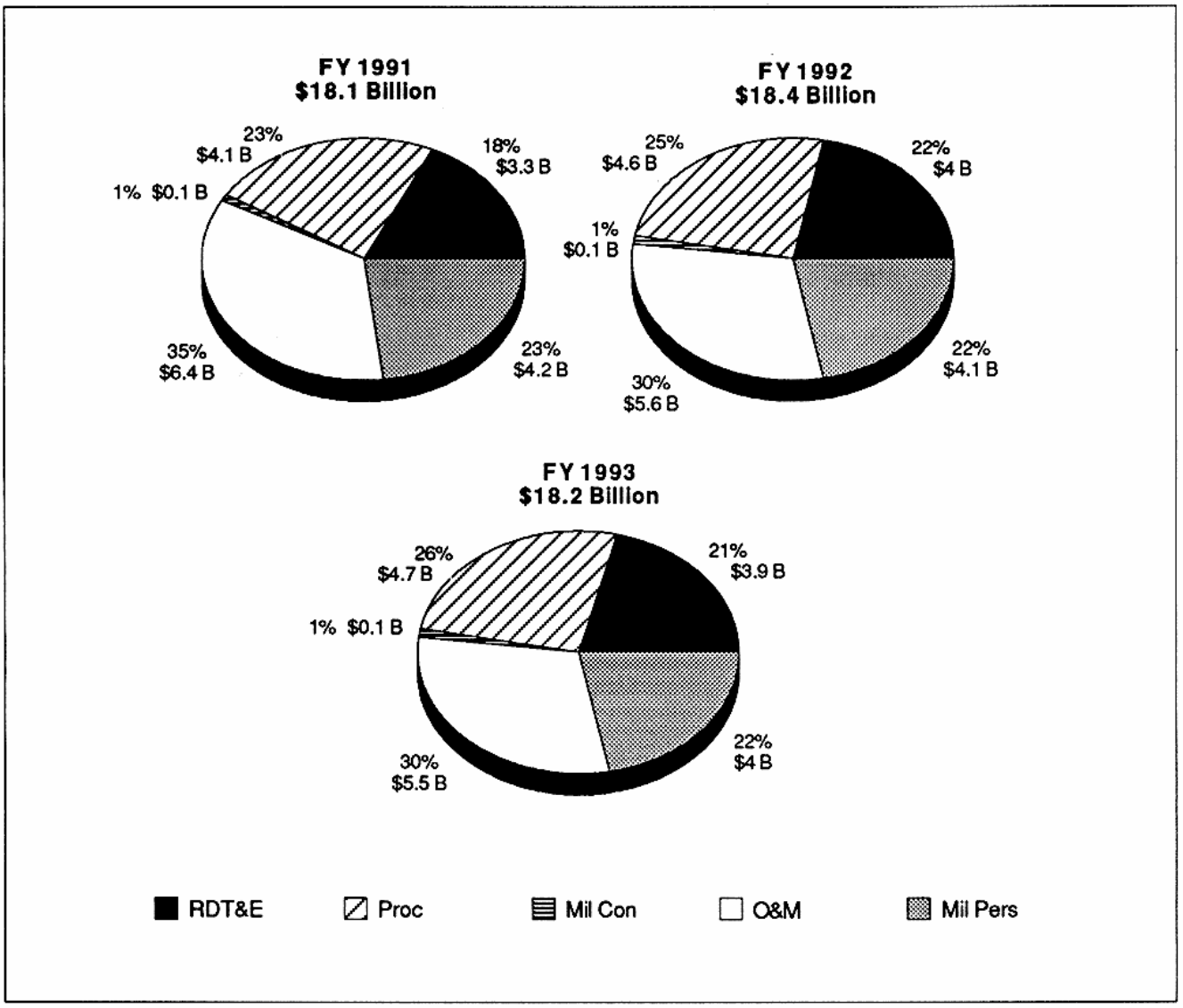

Figure 3
C^3 Resources by Appropriation ($ In Billions)

and how much they cost, collectively. What C^3I systems do is a little bit harder. It's an issue that I'm sure some of your other guests have grappled with. I think, unofficially, it's the capability we need to plan the warfare missions; to coordinate the use of weapons, platforms, and arms; and the ability to communicate orders and responses to the executors. As I said earlier, we tend to see C^3I as one step higher in the hierarchy than the actual weapons systems operations themselves: it is what it takes to plan a mission rather than to carry out the mission. From that perspective, the type of systems that we have bought and are operating tend to make some sense. If you try to look at them from the real mix of cats and dogs involved, it's obvious that any careful analysis will not show a direct correlation between what I showed you in dollars and my working definition, because there just isn't that clear a definition among all the practitioners. It's one of those things where the practicalities take over. Squad radios — the radios that 15 or 20 soldiers in the battlefield use to stay in touch with each other so that they can deploy to the right places — are typically in the C^3 budget. One could argue whether that's C^3 or not.

In general, I think the command end is easy to understand. The control end is a little bit harder. Some of us may have thought about C^3I seriously before the 1980s, but during the 1980s the concepts of C^3 and C^3I came into much more prominence, at least in the press, for one reason: the nuclear buildup and the nuclear threat. Control of nuclear weapons from the President (with his infamous little bag), down to the local commander is serious business. People don't release nuclear weapons based on rules or engagement or other types of standing orders; they have all been controlled, and I think there was a perception among the public and among our allies and others that no one released nuclear weapons based on anything except a very robust (and trustworthy) command and control system that is nuclear controlled.

But on the tactical end, with conventional weapons, that's never been the way we used the term "control". We've built command systems so that commanders can make educated decisions as best they can at their level, and pass the word down. We hope that we fight as we train and train as we fight (whichever way you'd like it), we have rules of engagement (ROEs) that cover the way in which weapons are to be employed and we don't have detailed control mechanisms. But if one particular platform or unit is given the command to engage enemy forces, each of the commanders of the proper echelon uses those systems that have been provided to him — sensors, radios, whatever he happens to have at that moment — to engage the weapons in the way he's been trained to use them under the rules of engagement, to deal with the situation as best he can, and eventually the feedback will get back to the proper levels of command, who will decide what the next orders need to be, based on how well the first set was carried out.

In Southeast Asia during the late 1960s there was a perception that President-to-foxhole types of orders were issued. I don't think DOD ever believed that. There might be people around who saw it, but we would think there's very little that the President would have to say to someone who is down at that lower echelon of command, because there's just not any common understanding of what's going on or what resources are available. We have intermediate levels of command for reasonable purposes, and the information is available to those people who are closer to the action.

Philosophically, that division between nuclear and conventional went on for quite some time. It started to change somewhat, especially in the mid-1980s, when we began getting into things like increases in the number of tactical nuclear weapons and additional classes of dual-capable delivery systems, which are weapons platforms that can deliver either nuclear weapons or conventional weapons. Of course, with additional nuclear capabilities, its concept of control started grinding itself further down in the command structure.

I want to give one quick illustration about the practicalities of command and control. In 1967, when I was working for the Air Force, we were putting together a tactical switching system that was to be used in Vietnam. It was one of the first automated telephone-type systems put out with the troops. It took advantage of the solid-state devices that had recently become available. Typically, telephone switches, as you know, are in brick and concrete buildings like the ones across the street, and people who program them or join the wires together know where they are in the hierarchy, that is, where to find the 471-exchange if you dial from the 472-exchange. Telephone exchanges are pretty well nailed down in most commercial environments. In the tactical environment, where you put one in the back of a truck and are going to drive it around, obviously one telephone switch has to have some idea where the others are; otherwise it's kind of hard to complete a telephone call to the proper person. We literally decided to leave two wires sticking out of the side of this van, and labeled them as "command and control" because in 1967 other than by looking at a piece of plexiglass with grease pencil entries, there was no real way in any automated sense, or any other sense, to find out where Battalion 7 of the Third Marines might happen to be on Thursday. It really turned out reasonably well when the operators got those switches, they designed some "workarounds," and made it work out of necessity. However, from my personal opinion about C^3 and command and control that's where DOD was in 1967 — a set of wires going noplace.

To go back to the unofficial title, I was going to talk about "C^3I in Transition." I've tried to build up to a definition of C^3 and where we are now and where we might be going. That sort of meets my definition of "transition."

Now, the question is how we build C^3 systems. I think overcoming the threat has always been part of why C^3 is different than say building telephone switches for the New England Telephone Company or computers for your lab. We've had several threats which we tried to take cognizance of. The first one, I think, is the vulnerability of the physical system.

That's pretty obvious. When one goes to war, things will get blown away, including C^3 systems, along with weapons — and people, unfortunately. But if a C^3 system really is part of the way we do business, and the way we need to run our forces, and we depend on it for those purposes, the commander won't be very happy when it goes away. Therefore, it needs to have some degree of physical protection, not just the actual hardening of the centers or mobility, or whatever else you might do to keep your C^3 system from being blown away by the enemy, but also protection against being disrupted by electromagnetic media, being jammed, or electronically interfered with by EMP — the electromagnetic pulses that go off because of nuclear weapons release. Presumably C^3 system designers have thought about that, and increased their costs.

The trade press pushes the use of commercial off-the-shelf, nondevelopmental items; COTS is the normal name. Of course, one can put together C^3I architectures that are so redundant and so well connected or robust, that if half the network were to get blown away, the other half would still function. That's certainly one way to overcome vulnerability, but it's not the way we've done it in the past, quite frankly. We might do it that way in the future. Some particular applications might work well that way, but being more traditional, we've decided to pour lots of concrete to harden some facilities and then to make other things mobile so we can move them from high-threat areas. So, we've engineered against that threat of physical vulnerability.

The other threat you probably won't hear about from most designers, but the number one threat (or number two, depending on how you rank them), is that the C^3 system may be out of limits for timeliness, accuracy, and usefulness. If you put a C^3 system together, and you really trust it, you have to worry about it going the way your PCs occasionally do at school. It may be just the old garbage in, garbage out syndrome. If there's garbage in the system, then it's not of much use to a commander. Then there's noncompatibility: from the wrong disk size, to the wrong file structure, to the wrong application program. There are inept translations, and confusion, and we could tell stories about that. They come about not only because of our own ineptness or lack of forethought on how the system's going to be used, but also because the enemy may spoof by putting false messages out and giving out bad information. We talk about the "fog of war"; it's an overused term. In terms of computers, you might have seen some April Fool's Day newspaper editions saying that the Iraqis were provided a computer printer complete with a computer virus. That's kind of far-fetched, but obviously if one had access to the enemy's computer, viruses and things of that nature could be propagated.

Student: I guess you did succeed in neutralizing the communication system, not necessarily by a computer virus, but some other device. One of the men who came here to address us hinted at the possibility that this was the way they'd be trying to neutralize the communications system, just in general.

Lubarsky: Communications systems that use radio frequencies are a lot easier to disrupt than things that are hard-wired together. But both are possible.

Student: Especially during war.

Lubarsky: Yes, radio frequency jamming, of course, is one of our key topics. Given the vulnerability of the system to disruption of the electromagnetic media, if we jam a receiver, obviously it becomes less useful. The thing I talked about here is spoofing — where false reports are given on the air to influence enemy thinking; i.e., that a particular military unit is heading east when it's really heading west. Electronic cover and deception is practiced by all military units. One of the vulnerabilities in the C^3 systems is that you can't believe everything that is reported, because even when it's reported by friendly forces it may be as a result of a well-laid deception. In the old days that was harder to do, because it didn't propagate as fast. One observer with a pair of binoculars saw something and reported it to his superior and that was it. Today, with interconnected networks, one false report gets on the net and it can wind up anyplace from the White House to the squad leader. So, as C^3 systems become more richly connected, one of the problems is that they are also more vulnerable to being spoofed and tricked and deceived and perhaps even attacked by viruses, although I don't personally know of any case of the last item.

Student: Does the virus story have some truth in it?

Lubarsky: I really don't have any way of checking. People don't usually brag about those things. We understand that it was first printed in a computer magazine as a joke and was later picked up by the trade press. Just from a technological and operational aspect, trying to propagate a virus into a full

C^3 network from a printer would be a pretty difficult way to operate. I leave that to the technologists, but I personally don't have any direct knowledge of it. However, in the future, obviously, people will be thinking about attacking that problem, including people in the U.S. government.

Oettinger: Up to this point, except for your charts where you differentiated between tactical, strategic, and so on, you've been speaking pretty generically. Do you intend to differentiate a little bit among these various areas in terms of what's going on? What happens at the nuclear end is, I would imagine, considerably different from what you need to do in counternarcotics, and tactical is sort of in between.

Lubarsky: I'm hoping to get to a little bit about that, certainly. I think I've gotten through two of the threats — the vulnerability, physical and otherwise, and the questions of limited timeliness and accuracy and usefulness. The fourth item, of course, is if we really think a C^3 system is worth anything, we have to worry about technology transfer, compromise of operational matters, communications security, tapping phones, and eavesdropping. I think you all realize that the largest compromise we've had of classified information in the recent history of the Department of Defense was by people who were part of the C^3I system, unfortunately. We don't brag about that, but in the Walker and Wentworth case that I'm sure you're all aware of, they had access to information that was available primarily to people employed in the innards of the C^3I system. The actual numbers of spy cases over the last 20 years that involved C^3I system operators is classified for one reason or another, but I can assure you it's a sizable percentage. The most attractive targets for any enemy espionage apparatus are those people who work in C^3I and typically have access to much more information than others.

Student: It's like Willie Sutton.

Lubarsky: That's exactly right. So we really do have to worry about compromises, leaks, and technology transfer. Again, commercial equipment doesn't always help a lot for that sort of thing, even though people say we should push more commercial equipment.

Just to end my short treatise on threat, the typical Soviet doctrine was to get rid of a third of the C^3 system by blowing it up — physical destruction; to jam one-third with electronic equipment that the Soviets called radio-electronic combat (REC); and to let the other third of the C^3 system go away, because it won't be of much use to anyone. The Egyptians followed that doctrine very well in 1974 against the Israelis. The Israelis overcame the jamming eventually, but it really made a difference. The Iraqis, who we assumed would have the same Soviet doctrine and ideas, and access to the same Soviet jamming equipment, did not follow it. That's on public record. Whether they didn't have the will, or didn't think it would help their tactics, or whatever, I'm not in a position to say, but it just didn't happen. Whether the Iraqis would have been more effective had they tried to disrupt our C^3I systems is unknown. We relied on a lot of commercial communications, and a lot of other commercial C^3I systems in Desert Storm that were vulnerable to various countermeasures. They weren't attacked.

I just want to say one word about intelligence, and the intelligence input to the command and control system. I think you're going to have several guests involved in the intelligence community here. Rich Haver is still coming, I suppose?

Oettinger: He was here last week, and Dick Kerr is coming next week.

Lubarsky: So you do have the experts coming. I'm certainly not one, but there is, obviously, a relationship between C^3 and me. We use it together in the same acronym. Intelligence is part of the C^3 system. It's part of what makes the commander aware of his options and how he might carry them out. A lot of the intelligence people don't like C^3 as a term; they use the term "battle management" to talk about C^3. I find that to be about the worst possible oxymoron. Anybody who thinks he can exercise supervisory control over a battle shouldn't bother fighting the battle, because the other fellow must know that too. Just as an aside, the SDI (Strategic Defense Initiative) people like "battle management," because their idea of battle management is trying to shoot down weapons that have already been released. Therefore, you can more rightfully call it engagement management, but it just doesn't have the ring.

Oettinger: It sounds like a consulting firm.

Lubarsky: Right: Engagement Management, Inc. But battle management is a euphemism. It's currently being used by a lot of intelligence people. You see, to some critics C^3 doesn't really exist. There's only intelligence and information and battle management; C^3 is a figment of somebody's imagination left over from the 1980s. You may hear some of that. Obviously that's one way of looking at the C^3I problem.

Oettinger: Excuse me, from where you sit, why this perpetual nitpicking over definitions? My inclination, when I find something that looks counterproductive on the surface continuing all the time, is to assume it must be functional, because people aren't that stupid. So why is it functional? What do people gain out of this? Is it budget battles, turf, or what?

Lubarsky: I think, perhaps, it's control in the broadest sense of the word. The place to be in a military organization is with the commander, because people who are in command are the leaders and those people who aspire to be leaders want to be in command. They probably think that the people who are closest to the commander, who are the trusted advisors of the commander, who provide the systems and the information and the services that help the commander do his job best and are found to be true believers, tend to gravitate toward the top of the system and will get the biggest part of the budget and the greatest percentage of the promotions. It would be hard to track that statistically, but that is the perception. I think these arguments go on for all the reasons you mentioned — budget, control, accessibility. Is the J2 closer to the CINC than the J6, the J6 being the communicator and the J2 being the intelligence officer? Who has the biggest office and the one closest to the CO? I think it pervades down.

The intelligence community has its own congressional committees. We all realize that there are eight committees now in the Congress that pass on those numbers that we talked about. Traditionally, we had an armed services committee in the Senate and the House that decided what DOD should do, and we had an appropriations committee that had subcommittees on defense. After the Watergate fiasco, the intelligence community came under the oversight of two new committees (in the House and the Senate). Now we also have a budget committee that determines the total breakdown between DOD and non-DOD budgets. In order to change (reprogram) one system from strategic to tactical, in the worst case, eight committees or subcommittees of our Congress have to approve a $2 million transfer of funds. I don't say that to be critical of the Congress. Not everything, of course, falls under each of the eight committees, but a lot of things that I personally work on do need approval of six committees (or subcommittees) to be accomplished. So it's not far-fetched.

Oettinger: Given the current mood in the Congress, aren't you having to cut back on personnel and equipment to hold costs down?

Lubarsky: As you know, most of our C³I assets, in the case of land forces, have been invested in preparing to fight the battle of the Fulda Gap. Most of our troops that aren't in the United States are in Europe, although there are some in Korea. The tactical forces, in general, and the C³I equipment we talked about for the tactical forces, have been procured to keep our land forces in Europe competitive with the Soviet-Warsaw Pact threat, which has always been numerically superior in force-level and superior perhaps, in quantity of weapons systems. So that's basically where the money has gone for the Army, in a macro sense.

Under the Conventional Forces in Europe (CFE) treaty we decided to move a lot of people out of Central Europe even before the Berlin Wall started falling down. Additionally, we found when we started counting people in Europe, many were intelligence people, ADP operators, and communicators. Obviously, we wanted to move them out first, so they're leaving in large numbers. Several signal brigades are coming back. We're leaving Central Europe as a tactical C³I "wasteland," of sorts, with some provisions for reestablishment.

If we should have to reinforce Europe again, we're going to have to bring the equipment back with us. Many of the fixed C³I systems in Europe were old; some we had even inherited from the Germans in World War II, and we were just getting around to replacing them in the 1980s. Our theorists say we could put together networks that are different from what we used in Europe for tactical purposes, and we'd take advantage of modern technology of different types. We should be putting together networks in Europe that will support the smaller forces we're going to have there, as well as coalition warfare, which may, in fact, include part-time allies — maybe the Hungarians, who want very badly to be in NATO in some sense, or the Romanians, perhaps. But obviously there are means with new technology to let everyone in the network for peacekeeping, perhaps, so that we can keep track of each other, and also to fight a war. We have communications security and computer security technology that would do that, but it's not being done at the moment as far as I can tell. We're taking the 1960's technology that we built in the late 1970s, early 1980s, back with us, parking it in truck parks or assigning it to the National Guard. CFE was moving

us out fast enough and now that the budget crunch is coming, we're going to move out even faster.

We talked about jamming being a big threat. We started building antijam radios a long time ago, and the Army inventory objective for SINCGARS (single channel ground to air radio system) which is one of DOD's small ($10,000) radios, started off at about 465,000 radios. I think we're down to maybe buying 170,000 now; we may only buy 70,000 or 80,000. We do have two sources and two production lines, one in Ft. Wayne, Indiana, and one in Tallahassee, Florida, to build them. We know what technology we'd like to have; unfortunately, we're in a state of transition, have a limited amount of new technology currently in production, and are downsizing.

Nuclear C^3 systems, of course, have always been very expensive to operate. We've kept the airborne command posts up as I'm sure you know from the open press. We don't talk about it much, but each of the nuclear capable CINCs has had command posts — typically 707s — either orbiting or on the runway ready to orbit in case there's some indication that nuclear weapons might be employed. They're a 1960ish design. With Congress's help, we're talking about cutting back the number of airborne command posts that are in the air at one time, replacing them with some unified command posts, and using more modern aircraft that are cheaper to operate. But in general, you saw the strategic costs up there (figure 2), and they're not changing a lot. It's cost us a third of the C^3 budget to run the nuclear, strategic C^3 system. The triad is still here: we still have nuclear submarines, nuclear equipped bombers, and land-based missiles. There are fewer as we start to downsize those forces, but as long as we have one of each, unfortunately, the nuclear C^3 system has to be around to send the EAM, the emergency action message, which triggers a nuclear response. Whether you're going to send it to one submarine whose location may be anywhere in the world or 200, the difference in cost to the C^3I system is inconsequential. You're going to have people orbiting ready to transmit the message. We've never trusted EAMs to a single communications link; we've always had sensors with dual phenomenology, so before we declare a missile launch, we have several indications from various sensors, whether they be IR (infrared), or radar, or whatever, that one was being launched, and was coming either toward us or toward a friendly nation.

Targeting the SIOP — the single integrated operations plan — is a big job even with modern-day computers. One does planning, which takes forever, and every time somebody changes a name from Leningrad to St. Petersburg and back again, we have to change the SIOP. It's not a trivial problem, regardless of what someone with a Cray computer in the lab thinks. These are ingress and egress routes and one has to do it under stress, obviously, and be prepared to do it under stress. The C^3 system isn't worth much unless you have some idea that if, in fact, it is ever needed — obviously everybody hopes it's not — it had better work, and the only way to make things work is to update them and change them, practice, do all the alerts, send all the 500 or so practice messages we send over a period of time. So finally, to answer your question directly, Dr. Oettinger, even though we're cutting back on some of the R&D in the strategic area, and on some of the procurement on sensors, and on the fixed costs of military personnel, the operations cost is still there and I don't see it going away.

Usually, when we define our C^3 architecture, it is based on our organizational concept. We have a Joint Staff; we have 11 CINCs; they have command centers; they have support units, which I think you've all been exposed to. They have fixed ops plans, in general. They were designed to run on large Honeywell mainframe computers. They're second generation: designed in the 1960s, but have been updated over the years. Without telling tales out of school, we have computers in Cheyenne Mountain whose compilers have supposedly been lost, so we can't even write any new code for them. That is probably the worst case. For the others, it just takes lots of time to update them.

Now, the question is what to do about this very nebulous threat. Iraq was a fairly large threat. We hope that in the future the types of operations that DOD will be called upon to carry out will be a lot smaller, in general. In case of a larger operation we depend upon the Reserves for much of the support units. If the President has the political will to issue the first order, "Call up 200,000 reserves," there's a pretty good chance that whatever DOD is called upon to do will in fact be what a large segment of the public would like done, and not something that can be blamed singly on the Congress or the nebulous bureaucrats or the military establishment. I think we learned that from Vietnam, and so far we've learned it well. If most of the support for large operations is in the reserves, and we can't resole our boots without a reserve shoe-manufacturing battalion there, and you'll be all set. That's an overstatement, but it's really where we're going; the question is how much of the C^3I infrastructure can be transferred to inactive status.

McLaughlin: Isn't that dangerous in the other sense, that that was the Army plan pre-Vietnam? Put the critical support in the reserves and the President would have to activate them?

Lubarsky: Yes, and it worked out poorly in Vietnam; but since then we have done better.

The next thing I was going to talk about is the war on drugs and what DOD has done about it, only as an illustration of what the low end of C^3 looks like.

McLaughlin: Fuzzbusters?

Lubarsky: Right. First of all, I don't know if a university campus in Boston is the right place to talk about what your federal government is doing to stop the threat of drugs, but I'll be fearless.

Oettinger: It's best in Oxford, where it doesn't violate any American federal or state laws. That's a nonpolitical statement.

McLaughlin: Whether you inhale or not, right?

Lubarsky: We won't make everybody here take a drug test before we do this. You know all DOD contractors now do have mandatory drug testing provisions, at least randomly, and we are coming out with the Executive Order as we speak to implement that. But you'll see that the federal government in 1991, which is the last year I have decent numbers for, was spending about $10 billion directly to do something about what we think is the drug threat, and out of that, DOD is spending $1 billion (figure 4). You can see there are lots of organizations here, and the reason I show that is to let you know that it's not a military-only war, and DOD's not in charge.

By congressional legislation in 1989, DOD got stuck with about four things to do (figure 5). We're trying to support friendly foreign governments — maybe some of them are not so friendly, but we get along with them — to prevent drug exports. We're trying to assist those law enforcement agencies that have the responsibility to keep people from shipping

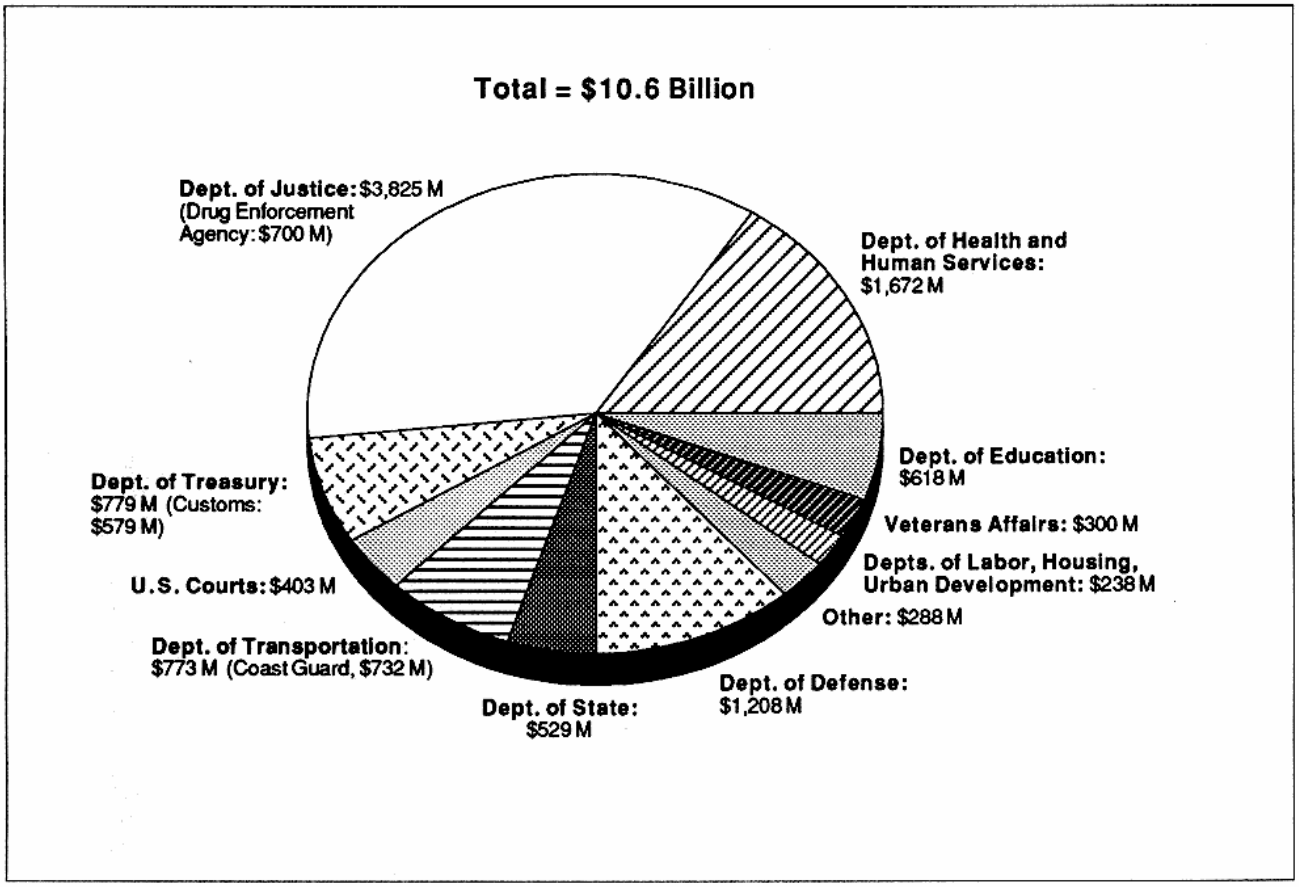

Figure 4
The DOD Drug Control Program
(The National Program, Fiscal Year 1991)

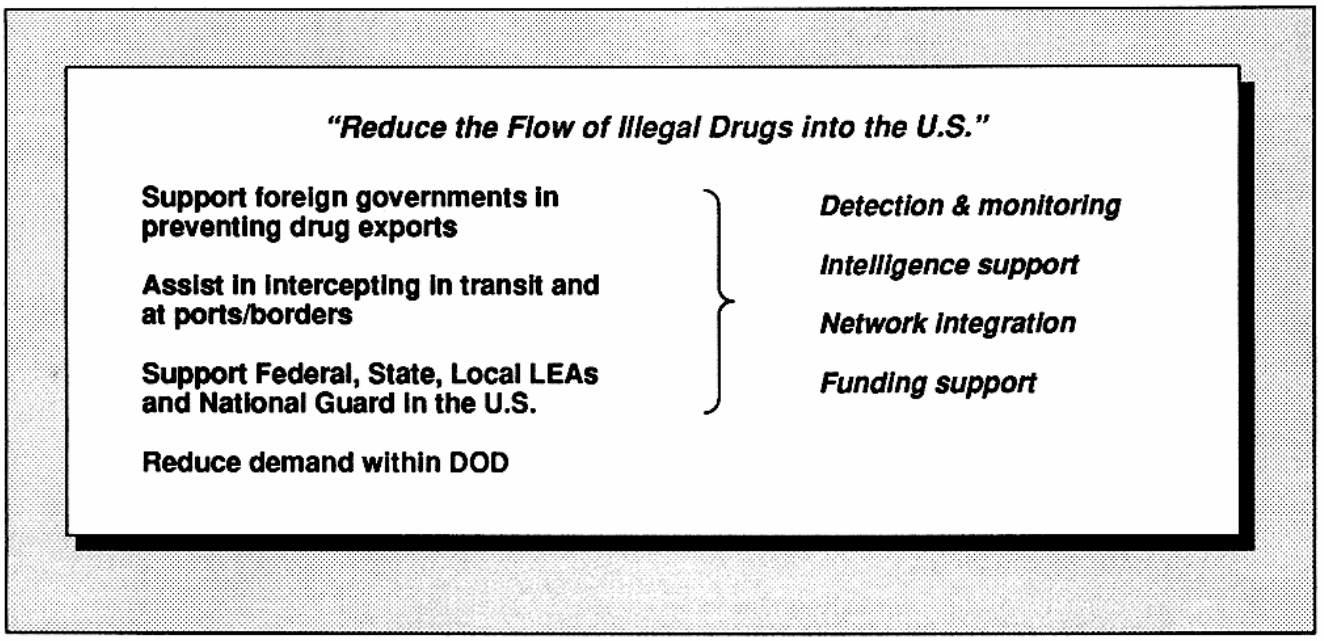

Figure 5
Our Approach: DOD's Role

drugs into the United States, and we're supporting the federal, state, and local law enforcement administrations (LEAs is our abbreviation; typically you see it with an F in front of it, which means federal; and S&L, which means state and local, not banks — we try not to use the other S&L, obviously), and the National Guard. And, like all good citizens of the country, we are reducing the demand for drugs within the DOD community, and in truth we are.

The major problem over the years, the way DOD has seen it anyway, is that people are smuggling cocaine from Central America into the United States by various routes (figure 6). We have about 140,000 private vessels that show up in the United States in any particular year, about 100,000 commercial vessels, about 3 million large ISO (International Standards Organization) cargo containers, and about 5 million people who kind of wander around and show up in the United States and leave again. These are all estimates. If you go to the intelligence community, CIA has a set, and so do other people; these are the ballpark numbers. Obviously, people have a propensity to try to bring in cocaine because there's a large markup. It's easier than smuggling Mercedes and other things that people are used to smuggling.

What has DOD done in intercepting transit in ports (figure 7)? I think I promised some of the people at lunch a picture of a balloon; that thing there at the upper right is about a 270-foot aerostat, as we call it, tethered to the back of a sea-going boat that we lease from companies that typically tend oil wells on Texas towers. That picture in the middle is supposed to be a Coast Guard cutter with some radars, and below that is our famous AWACS. This is a sort of cutaway of a tropical (you can see it's tropical; it has palm trees) radar site that we built down country, so in transit we're trying to track airplanes and ships that are coming into the United States over those routes that I've just shown you (figure 6). Of course, the drug traffickers don't have fixed operations plans. They don't have to call up the reserves. They don't have CINCs with mainframes. What they do when we close one of those arrows that I showed you is to find another arrow, and come in some other way. You may be aware that the original threat was people just taking small planes and flying into Florida. We figured out how to fix that in a rush, and now flying a plane of any size directly from Central America to Florida while avoiding detection is very difficult. We put up what we call "condo radars" on top of the tall buildings that line the eastern coast of Florida. We put little radar sets up on top, which are very cheap to operate and along with the Customs Service, kept track of airplanes coming into Florida. It's a very simple job, as it turns out. There were also some AWACS orbiting, a few Coast Guard cutters and U.S. Navy

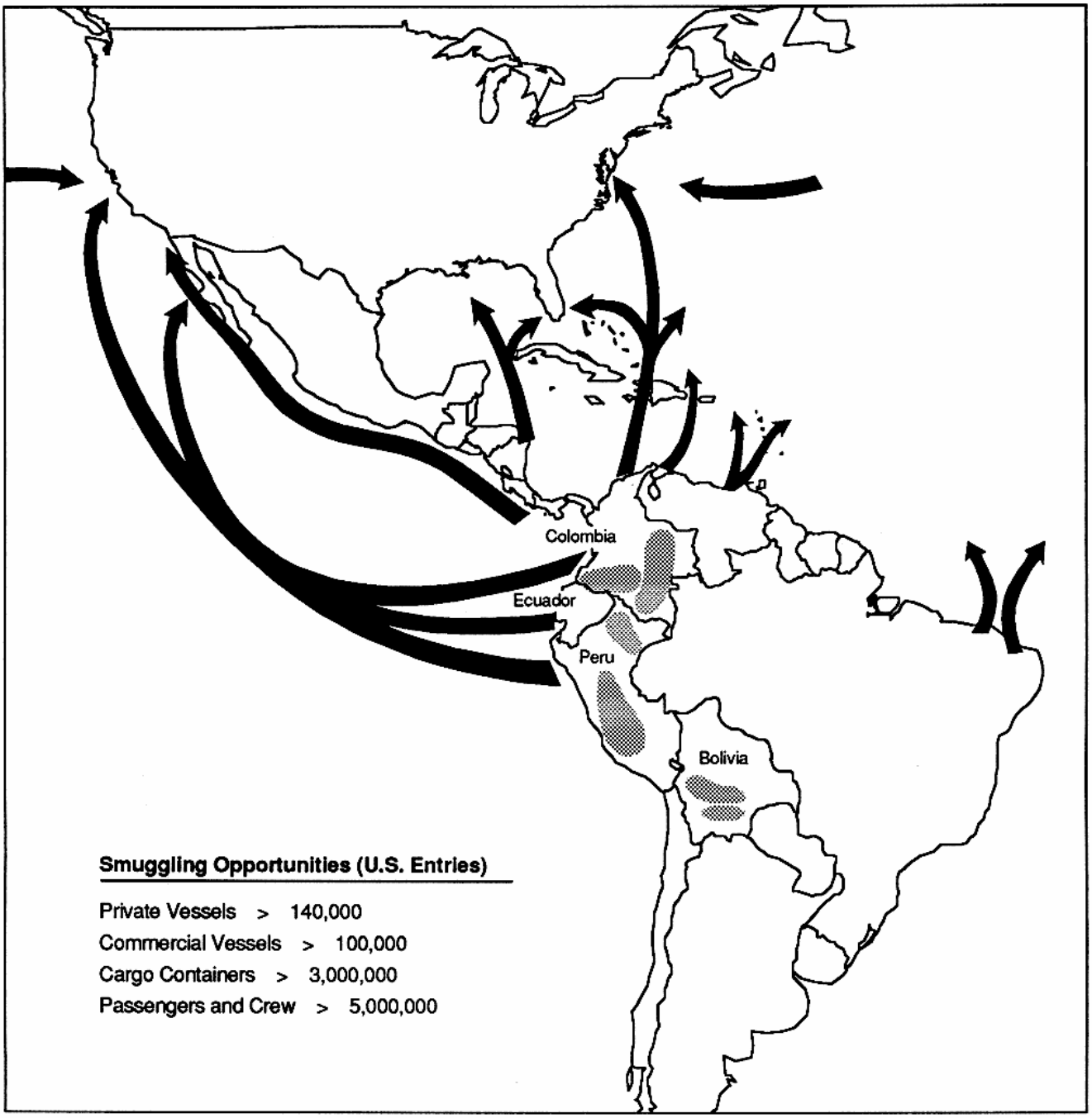

Figure 6
The Problem:
Cocaine Smuggling Routes (Maritime)

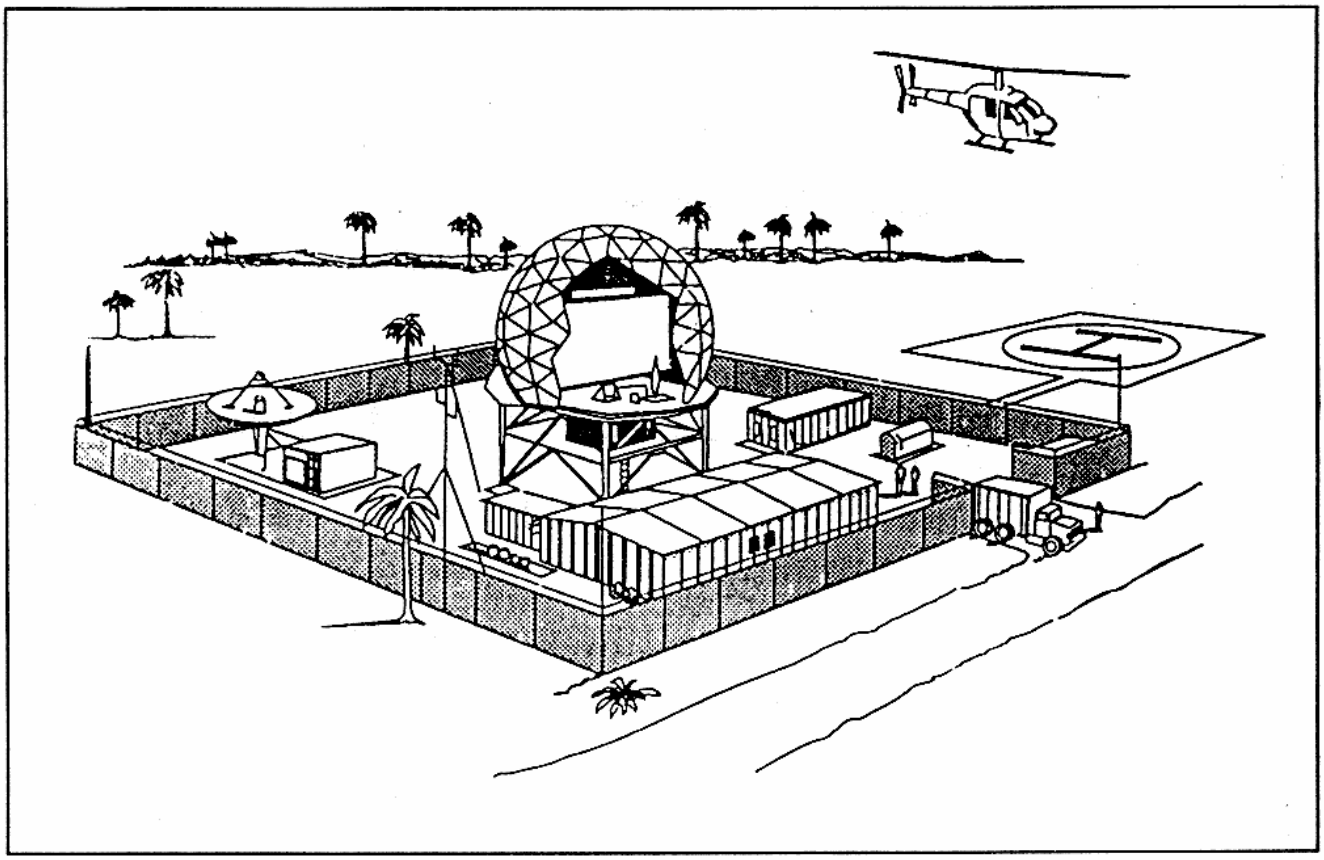

Figure 7
The DOD Drug Program:
Assist in Intercepting in Transit and at Ports/Borders

destroyers out, and a few ships with aerostats on them.

Student: What does the balloon do?

Lubarsky: The balloon has a $2.6 million Westinghouse F-16 radar set on the bottom of it. The reason we put it in a balloon, of course, is that microwave radars are basically line-of-sight devices, so if you put them up at 5,000 or 6,000 feet, the distance at which they can detect airplanes is a lot longer than if we tried to keep them on the deck of a ship, where they're at sea level. So the balloon hauls up a radar set, and the radar spins around. We put an ESM (electronic support measure) receiver up there, so if the pilot of the plane turns on his radio transmitter and tells somebody who he is, we can also hear him.

Student: Just out of curiosity, why did the government decide to get the military involved in it? It sounds as though it's because there's equipment in it. But why can't civilians do the same thing? It seems that it gets rid of so many problems.

Lubarsky: That's a good question. Well, of course, the answer I got from Chairman Murtha, of the Defense Subcommittee of the House Appropriations Committee (HAC) directly at the hearing yesterday, is that they thought that DOD had the expertise to do it. The problem with the LEAs is that they are composed of career policemen or lawyers; they don't have the background (in most cases) to run large involved radar nets, computer networks, the intelligence collection that DOD routinely handles. As I showed you in the original slide (figure 4), DOD is not the only one involved; we only had one billion of the ten billion dollars. That's why I showed you that first; there's a perception that DOD's the only one doing counternarcotics. That's certainly not the case. We're 10 percent of the federal effort, by budget.

Student: But to follow up on that question, I thought that one of the original purposes of DOD's being in the game was to provide C^3 expertise, and I wondered whether you have been successful in that.

Lubarsky: Yes, and we're going to talk about that. I was trying to work to that and look at the pictures first.

Tracking aircraft has been easy. You can talk to law enforcement officials who have other opinions, but that threat really has been overcome. However, as I mentioned, the traffickers have also changed routes. Now they fly up to some place in the wide blue ocean where it's a little bit harder for us to maintain full-time aircraft surveillance and drop the cocaine out of the back of the airplane without any sophisticated means — a rubber life raft or a submerged equivalent of a mine or a buoy — and come back two days later with a boat and a good chart and pick up the cocaine and run it ashore. So obviously, building better radars is not the full answer.

What we're trying to do is make it increasingly difficult for large cocaine cartels to operate. I think that's all DOD can ever hope to do. The government at present sees that the cocaine cartels, with a lot of money in a few hands, are destabilizing to local governments in Central and South America and are doing other things that we're against. So we're trying to force the cartels to change their modus-operandi, so to speak, to make it more difficult for them to bring cocaine in. It's very debatable as to whether the interdiction process is working. The measures of effectiveness are difficult and Congress said yesterday that their figures show that cocaine on the streets of New York is no more expensive than it was before DOD got involved, maybe even cheaper. Our comeback is that price isn't the only objective of this game. But it's difficult to determine success.

What are we doing? In this slide (figure 8), OPTEMPO refers to the tempo at which we operate ships and warning aircraft. CBRN is the Caribbean Basin Radar Network — we're building radars down to the Andes. I showed you a schematic of a radar with palm trees (figure 7). We're increasing coverage on the southwest border by putting in sensors and fences along the border so that people don't swarm across without having a chance of being intercepted. Over-the-horizon radar is a technology for longer distance detection, using HF (high-frequency) propagation rather than microwaves to track aircraft. We're trying to get better intelligence and, in general, that's how we keep track of drugs coming in.

I'll talk about the C^3 network very briefly. That slide's really alphabet soup (figure 9). As of about a year ago, those were the major players in DOD and related command centers that were involved in the war on drugs. Some of those command centers belong to the intelligence community, some to the Coast Guard, some to Customs, some to the FAA (Federal Aviation Administration), and some to a group of other people — in general, to the State Department. DOD's idea was to tie those command centers and operational centers together with a responsive command and control network, so if the FAA held various targets and aircraft, they could transfer the data around and we could get it to the right places. This figure is probably a little more disjointed than it ought to be, but DOD's expertise is in building networks, and we have put together a network with about 150 locations throughout the United States, Central America, and aboard Coast Guard cutters and other places. Everything needs a nomenclature; it's called ADNET, the antidrug network. We operate over a digital data system that belongs to DOD. That's what we've done to integrate C^3 networks.

The other thing we found out through doing business with the LEAs is that they all use radios that are transmitting in the clear, and, therefore, drug people who have access to things like scanners typically knew what was going to happen before the law enforcement people got around to them. So in 1989 we started to secure the radios used by all the federal agencies that are involved in the war on drugs, and it turns out that the United States, as you're probably well aware, is not a single "police state" by any stretch of the imagination. There are nine or ten major police forces that operate just along the southwestern border of the United States, and there's no way for them to talk to each other, because even though they use similar equipment, they have different networks, their tactical radios (taxi-cab variety) are connected to different radio repeaters at sites in Louisiana and Mississippi and on mountain tops in Arizona, New Mexico, and Texas. In general, if you wanted to combine FBI, Customs Service, Border Patrol, Park Service, and everyone else who might have some jurisdiction and help the State Police out in those areas, it just couldn't be done. We have people with frequency plans and communications networks that don't interoperate; we have a tower on a mountain in New Mexico with one repeater on it used by the Border Patrol, and one for Customs agents, one for the FBI, and one for the DEA (Drug Enforcement Adminis-

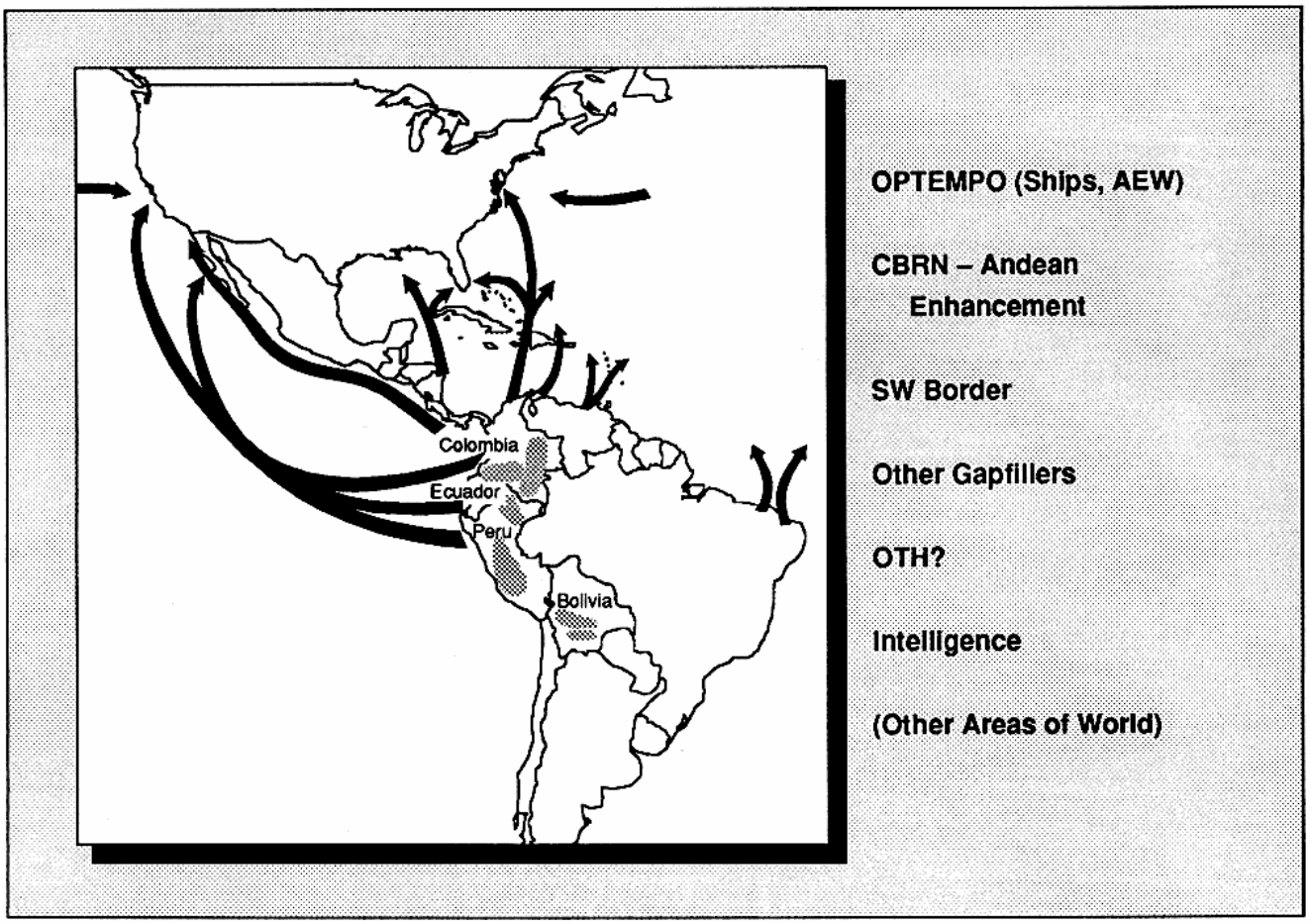

Figure 8
The DOD Drug Program:
Assist in Intercepting in Transit and at Port/Borders

tration), and as of a year ago there was no way to tie them all together for a joint operation. And they were all so "in the clear" so that even the least sophisticated person who is in the drug business would have no trouble using high-school-level techniques to intercept the communications.

Student: For the last ten days, probably because the Noriega drug trial is coming to a close, there have been a lot of specials in the news. Two of them — one with Dan Rather and one with CNN — discussed the command and control of the drug smugglers and said that we're having no success interdicting it and the smugglers are having a lot of success because they have a lot of money and they have access to some simple technology. I wonder what your comments are on that. You brought up the Bearcat scanner business.

Lubarsky: People are using better than Bearcat scanners. If you look through an electronics trade publication, lots of countries in the world are making rather sophisticated intercept receivers that are available on the general market for anybody who's got the price. Some of the DOD contractors are under limitations with export controls and things like that. We tend to keep track of the very high end stuff, but there is still plenty of good equipment available. So the answer is, yes, traffickers can keep track of our command and control in a lot of places, but there are ways to make it harder for them. Obviously, not every drug runner is Noriega; not every drug organization uses $35,000 intercept receivers to keep track of the Border Patrol, but some do. Some drug runners only have a Radio Shack one that costs $1,200, and those, of course, are easier for us to work around. But you're right.

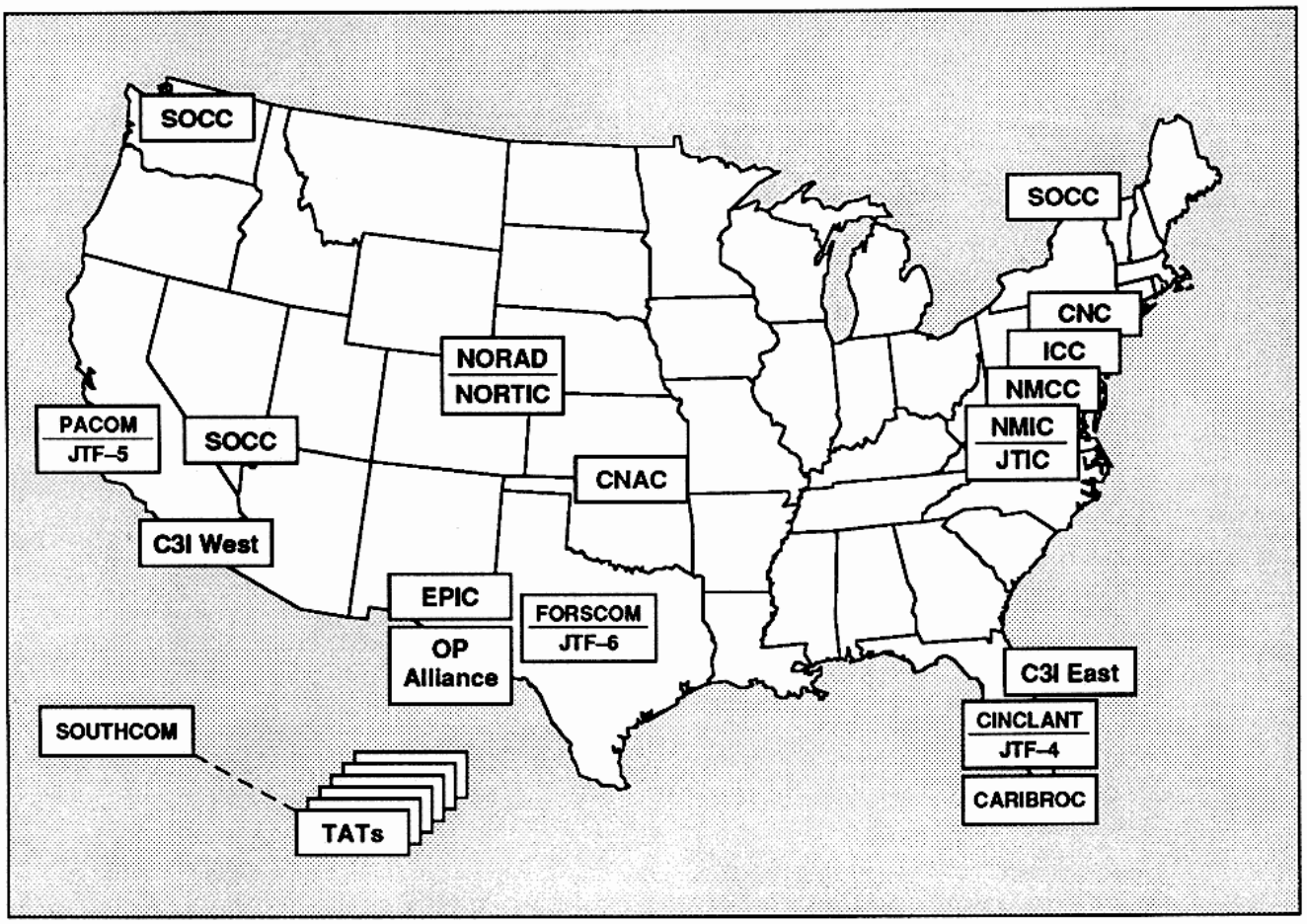

Figure 9
The DOD Drug Program:
Network Integration—Key Interdiction Centers

There's no question about it. There are technicians running around in lots of countries, with expertise on how to overcome DOD, and especially civil agency, C^3 systems. This talent is for sale.

The number one threat is the personnel problem. As I mentioned, we've had spy problems in DOD over the years but the civil agencies have very difficult problems. The easy way to find out whether a particular aircraft tail number is on the wanted list is to pay someone who earns about $20,000 a year and sits in front of a computer terminal all day to punch in the aircraft number against the latest list of wanted aircraft, and for $50,000 or so the drug runner now knows that his aircraft tail number is on the wanted list. So he either repaints the tail or finds another airplane or takes whatever action is appropriate. People doing that, in general, don't feel that they're aiding the enemy helping to "nuke" the United States. They're making $50,000 for doing something that's semi-bad, and sort of illegal.

Student: It seems that we've used the C^3I or whatever system in this case to try to treat a symptom, and it really doesn't address the problem.

Lubarsky: The problem is the demand. Obviously, if nobody in the United States wanted to buy drugs, then the problem would go away. We all understand that.

Student: Well, are we targeting the wrong thing? I mean, we're trying to target flights of airplanes. The drugs are the problem. It just doesn't sound right to me.

Lubarsky: We're going to break this thing down to simplistic terms: supply side and demand side. On the demand side the strategy is to encourage drug

testing, encourage young people not to use drugs, advertise, make it difficult to want to use drugs, and take some of the glamor away. I'm not an expert on the demand side, believe me. On the supply side, the idea is, of course, to make it more difficult to get drugs, number one, and number two, make sure that those people who want to use drugs take their business to the mom-and-pop store and not to large cartels, which we think are a destabilizing force in the world today. We really don't need drug money being funneled in large quantities to bring down friendly governments. So there is more than one level of sophistication.

I agree with you one hundred percent. Targeting ships and airplanes and containers is very difficult, but it's doable. But once the drugs, or people, for that matter, are in the United States, it's very difficult to track them. You know what the laws are in the United States; DOD doesn't have search-and-seizure powers. If you're coming into the United States as an alien, the federal government (not DOD) has lots of police power at the airports to do almost anything, including putting you back on the airplane for a return flight. U.S. citizens within the United States are obviously protected from those sorts of actions.

Oettinger: Before you go on, let me try to answer the question in a slightly different way, and then you may or may not wish to comment. The President of the United States made a commitment to engage in a war on drugs. He asked the Defense Department to participate. I think it's fair to say that in the early days there were some questions within the Defense Department about whether that was appropriate or not, including, given the history of some ventures like that in the past, making damn sure that if anybody wanted anything, there'd be a written order and that this would not be something where the military would later be the fall guys for using the military to do police work. I think two things happened. The President insisted, number one; and, number two, the objections regarding police work were partly overcome by this Balkanized structure, which makes multiservice jointness look like child's play. That pie chart you showed shows a degree of glomming things together that makes jointness look simple. So you have a political camel, which is, however, what the political leadership demanded.

Lubarsky: It's not only the President. The Congress directed in the 1989 defense appropriations bill that it be done. They said DOD will be lead agency for detecting and monitoring maritime and aircraft trafficking of drugs in the United States. It was directed in a public law. The Congress appropriates, obviously, and the President bought off on the job. We've had some Secretaries of Defense, as Professor Oettinger mentioned, who were not for it; however, the current one, being a creature of the Congress and other places, is for it and has pushed hard for it.

I didn't want to give you the wrong impression: that DOD was involved in doing "police-type" work. "Posse comitatus" actually only applies to the Army. It turns out that the Navy was exempt from that; the Navy can become policemen if they decide to, but the Navy doesn't do that for a good reason: the Executive Order. What we do in the case of actually making arrests is this: Navy ships in the Caribbean have LEA detachments on them, who are Coast Guard people. Coast Guard people are law enforcement officials. So when a ship is seized and boarded, the Coast Guard does it. This is not just for drugs. When we had an embargo in the Persian Gulf, the Navy found it necessary, under the same rules, to activate the Coast Guard, and the Coast Guard went to the Persian Gulf. The Navy tracks down ships and gets them to stop, but the people who actually jump aboard turn out to be Coast Guard personnel. They're the ones who are trained to do that kind of work.

Student: Do you think that tightening the borders and other things that are part of the counternarcotics program yield any significant counterterrorism benefits?

Lubarsky: The technology, as it turns out, tends to be somewhat the same. DOD's doing some of the R&D on containers, which is a difficult problem. As you know, containers pop up by the millions per port and you have to get them moving, otherwise commerce suffers. You cannot randomly search containers and do any good. The Customs Service receives the bills of lading and we have assisted them with some computer systems to do that. What we'd like to do is sniff them. Right now the best sniffer happens to be a dog, which is all right, but it's kind of slow and not exactly what we want. It turns out that some of the precursor chemicals used to process cocaine are very similar to the chemical content of various explosives. So we've kind of leap-frogged onto the same sorts of sensor technology that the counterterrorism people are interested in; we hope to come up with some mechanical way of sniffing containers and ships and things of that nature quickly and easily. But the technology is

really not here yet. We're talking about changing the ISO — the international standard — so that all containers would have to have some way of pressurizing and depressurizing, and we could blow something in the bottom and put a sniffer on the top and get the traces of the chemicals in there, both for products of use to terrorists and for narcotics. That would be an expensive change, but it is under consideration.

Student: I don't know your area of jurisdiction, but are your efforts confined to the smuggling end of drugs, or do they extend to the place from which the drugs are exported? I find the policy is rather conflicted. For instance, the finances of Afghan refugees are protected by the order of the U.S. government, but they are the greatest dealers of drugs, and I'm surprised.

Lubarsky: Fortunately, that's not one of the DOD's biggest problems. We do work with the Coast Guard (I've just spent some time out with them), and it turns out that illegal aliens coming from Asia in general at the moment happen to be a big threat, not only because they do bring drugs with them on occasion, but some of the people coming in that way are also people who would not normally be admitted to the United States. So some of this intelligence-type screening — which ships are coming, who's on them — we do share with them.

But you're right, that is one of the problems. We are helping at the source in those cases where countries with which we maintain friendly relations ask us to help. In South America and Central America, our Southern Command does aid friendly governments in stamping out cocaine at the source, and we train Colombian people how to get rid of crops and provide assistance to the local friendly governments. Colombia is very friendly. We've had on-again off-again relations with Peru. Guatemala and Nicaragua are usually pretty friendly. So they ask for assistance and we've provided them helicopters to move their police around and other things of that nature.

Obviously, we don't impose ourselves upon governments that don't desire assistance. In Southeast Asia at the moment, unfortunately, most of the governments are not on the friendliest terms with us and we know a lot of drugs originate in places like Burma, Thailand, and Cambodia, and come across the Pacific via ship. We do what we can to track such movements. Of course, most of the threat from Southeast Asia tends to be heroin, and much of the heroin, it turns out, is not destined for the United States. We've been pushing very hard on cocaine, again because of the political ramifications of the cocaine trade in Central America, because Central America is closer to home, very frankly, and enjoys more political attention in the United States than the nebulous sort of heroin trade from Southeast Asia. CINCPAC, our Pacific Commander, worries about ships coming across the Pacific. We're putting in spotter systems and computerized systems, as we speak, for a command center in Hawaii to track such movements.

Student: I want to ask you if there are either statutory or simply interagency problems with the use of communications or communications traffic analysis. As you said, they use Bearcat scanners on us; it seems that we have satellites and even more sophisticated things than Bearcat scanners or even the whole range of photoreconnaissance.

Lubarsky: The law is pretty specific about what we can do with that, and where it's legal and authorized by executive order, we certainly are doing it. I can't go into a lot of detail, but the civil agencies have some of that equipment doing HF intercepts on their own. Customs and other people do that, and NSA (National Security Agency), which does it for the Department of Defense, is engaged to a certain extent, but there are statutory limitations on what DOD, or any government agency, is allowed to do about intercepting private communications of U.S. citizens. As long as they're not U.S. citizens and they're outside the continental United States, and some other restrictions are met, we certainly do that. We fly lots of photorecce over South America. It's not a secret; we're flying down there all the time for friendly governments that want us to fly. We have the authority. You noticed some of those nodes there (figure 9); the CNC is the counternarcotics center, which is operated by the Director of Central Intelligence. So they're involved in this, and we do use those assets.

Student: In general, has the use of the whole panorama of intelligence assets been successful, and, if not, have the bottlenecks been simply inadequate use, statutory problems, or interagency problems, or is it simply not an effective tool?

Lubarsky: I was going to get back and talk about C^3 again, which is what I came to talk about. I think that in a C^3I system, the endgame typically is a battle or engagement that DOD sort of controls, and we use C^3 to decide which weapons to fire. The problem with this is we're providing C^3 to other

agencies that are the analogue of the weapons system. The people who do the intercept are Customs or Coast Guard, or Border Patrol, and it turns out that they're pretty asset-limited. My perception — I'm not sure it's their official position — is that we can give the LEAs more intercepts to pursue than they're ever likely to be able to handle. So, is the C^3 system doing a good job? Yes, but the C^3I system is not really well matched in some cases to the interdiction assets available for pursuit. So then we get to the problem of trying to help the civil agency sort out the most important targets, which ones they ought to go after first, and this gets to be a big pain, very frankly. It's hard for one agency (DOD) to tell others (LEAs) how they ought to operate, as you can probably guess. We're not good at it either, and DOD people tend to use fairly direct terms that don't always go over too well.

Student: But in a command and control sense, isn't what you're describing the model of coalition warfare?

Lubarsky: Certainly. It is to the nth degree, and if we can do this, we can do almost anything in C^3.

Oettinger: Well, maybe because there's no coalition, we're more intractable than we are friendly.

Lubarsky: We've so many people who are in charge in this thing. I think, in general, the C^3I system has some problems in providing information to our friendly law enforcement people. Number one, as you brought up earlier, is that DOD finds it very difficult to share a lot of the available information. The typical county sheriff doesn't have a security clearance. He probably doesn't even have a safe or a crypto box or anything else needed to handle classified information, so therefore we don't give him any. I'm sure you know what the rules are for classified. Even the lowest denominator of national security information, Confidential, has to be locked up, those to whom it is entrusted have some sort of background investigation to prove their citizenship, etc. That's not the case at all below the federal law enforcement agencies. Very few state people get involved.

So we have this big problem of sanitization, which in general means making sure that the information that is provided the local policeman can't be easily traced back to the sensor that gave it to us, especially if the existence of that sensor is not widely known. That's a problem when you put it on a network. We're trying to overcome that. We do various things to sanitize it and rename it. We put all these things together in one database and stir it around. We're getting together a system for the states of Alabama, Louisiana, and Mississippi called the Gulf States Initiative, where we're helping them tie together some of their computer databases so that they'll be able to share information in ways they couldn't before. I think the perception is that these law enforcement agencies have transparent boundaries. It's not the case. A lot of our states just don't share data very well, for policy reasons or technical reasons. Believe it or not, when you drive across some state borders, you're in another country because it's very difficult in a real-time sense to know whether you're even in a stolen car, let alone whether you're suspected of moving narcotics. We can feed information into shared systems such as these that comes from places we'd prefer not to acknowledge. Those things are doable, but they're hard.

The easiest thing we did, getting back to my original point, was help the LEAs secure their radios. Congress gave us permission to spend about $150 million to loan the federal law enforcement agencies secure radios and things, so we bought STU-IIIs — I think you're familiar with those — which are standard dial-up telephones that have a crypto device in them — ones that are difficult even for sophisticated drug traffickers to intercept. We put out about 9,000 or 10,000 secure telephones. Each of the U.S. Attorneys now has one, so if he wants to talk about a drug case with Justice, at least we know there is no chance of a drug person finding out about it from a phone tap. We've secured radios along the southwest border using a system that Motorola builds called "over-the-air rekeying"; now when an Immigration agent wants to get on the same net with DEA or the Park Service, we put some common nets together for him, using our great Army network engineering people. We now have common drug interdiction nets in Arizona and New Mexico, so an operation in Nogales for instance, can include all the federal and state people who would like to participate. It's very difficult for even a reasonably well equipped drug organization to know that the operation's going to happen and there can be people in the area ready to interdict the traffickers. Does all that help? That's a good question. We know that doing nothing sends entirely the wrong signal; we're sure of that, but I don't know if it can say that what we are doing is of great help. The LEAs need to judge that.

Again, because Frank [Snyder] and Professor Oettinger brought it up, this might be an example of

what the low end of C^3 is going to look like. We're going to have the same sort of problems when people in CSCE (Conference on Security and Cooperation in Europe) decide they're a part of NATO. We may have Hungarian divisions that want to protect themselves from the German army while both are our allies, which in our lifetime — or at least in your lifetime — may happen again.

McLaughlin: Turks and Germans.

Lubarsky: Right. They're not getting along this year. They were always famous enemies.

I think what we're learning is how to put together networks that are capable of handling various levels of private information, and, we hope, stirring it up well enough and popping it out so that the people who get it don't really know where it came from in excruciating detail. The technology is here. The other question is, do the bureaucrats who are in charge of all this want to make it happen? This is the low end. The high end is another matter, obviously. I'll just close by saying that if we don't do all these great things, I would project that in the 1990s we'll be back in the same place we were in the 1960s, where two wires emerged from the switching equipment were labeled as "C^3" and didn't have any place to go because there wasn't a responsive C^3 system. With that, I'm going to turn it over.

Oettinger: We're running out of time, but let me ask you a quick question. I'd like to bring you back to something quite different and get your comments on it because you have a span of experience that's unique. Within the last week or two, the United States and a number of other countries signed an "open skies" agreement, and it seems like just yesterday when speeches by the United States President about open skies were treated with some skepticism. Of course, the first implementation of it was kind of notorious, when the guy got shot down over the Soviet Union. It's only in the Carter Administration that the President of the United States officially admitted that there were satellites up there doing reconnaissance. Before that, while there was a lot of stuff in the press, nobody could ever even own up to the fact that it was happening, even though there had been books written. You've been a witness to most of that transition. Do you want to comment on what you see has happened, and how much difference it has made: that whole notion of open skies, from one sort of surreptitious U-2 to a treaty that says, "We're going to do it all over the place and everybody and his brother is now agreeing to it."

Lubarsky: I think in this case the policy and the treaty and the politics are following reality. The United States doesn't have a monopoly on this anymore. If you look at any reasonable photography that's being worked, you're going to see a little French acronym at the bottom that says "SPOT." (A French imaging satellite system, "Systeme Pour D'Observation de la Terre). It's just a matter of time until the CNNs of the world have their own satellite flying around and getting coverage. You may have seen reports about three weeks ago that there was an explosion on a ship doing some research for the Navy off the State of Washington. It was a contractor-owned and operated research ship. CNN had it on within 15 minutes and the Navy command system didn't know what was going on, very frankly, for quite some time. I think it's a prime example of where technology and reality have driven things to the point where it's ridiculous to keep your head in the sand forever. I think certain intelligence organizations, especially, have been guilty of this. There are people that refuse to admit it, but with the Russian lift capability, which is on the free world market now together with French, Chinese, and Japanese lifters, one can put up almost anything into space. There's technology around to build capable packages from the Japanese and European electronics industries. There's no way to stop it. These countries are saying that they're going to forgo doing really nasty things with open skies. It may turn out to be a treaty that is merely damage limiting. Obviously, that may not be the official DOD position. You can look at the photography in any recent paper on a crisis area and you'll see "SPOT" logos all over it.

Oettinger: Do we have any other questions? If not, then it remains for us to thank you for a fantastic presentation.

INCSEMINARS1992

ISBN-1-879716-16-X