*INCIDENTAL PAPER*

# Seminar on Intelligence, Command, and Control

## Information Systems Support to DOD and Beyond

**Albert J. Edmonds**

**Guest Presentations, Spring 1996**
James R. Clapper, Jr; Mark M. Lowenthal; Richard T. Reynolds; Julie J.C.H. Ryan; Arthur K. Cebrowski; John M. McConnell; Albert J. Edmonds; Martin C. Libicki; Robert A. Rosenberg

**January 1997**

*Program on Information Resources Policy*

***Center for Information Policy Research***

***Harvard University***

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

*Chairman*
Anthony G. Oettinger

*Managing Director*
John C. B. LeGates



E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-39-9 **I-97-1**

# Information Systems Support to DOD and Beyond

**Albert J. Edmonds**

*Lieutenant General Albert J. Edmonds is Director of the Defense Information Systems Agency and Manager of the National Communications System, with headquarters in Arlington, Virginia. He is responsible for providing command, control, communications, computers and intelligence ($C^4I$) support to the nation's warfighters. General Edmonds entered the Air Force in August 1964 and was commissioned upon graduation from Officer Training School, Lackland Air Force Base, Texas, in November 1964. He has held many critical $C^4I$ positions, including Deputy Chief of Staff for Communications-Computer Systems, Tactical Air Command (dual-hatted as commander, Air Force Communication Command's Tactical Communications Division); Assistant Chief of Staff, Systems for Command, Control, Communications and Computers, Air Force Headquarters; and Director, Command, Control, Communications and Computers Directorate (J-6), the Joint Staff.*

**Edmonds:** Let me just tell you it's a pleasure to be here. This is the third year I've come here to talk to a group like yours. What I'm going to do in my presentation, so that you get the benefit of my previous years of coming, is spend a little time up front setting the stage for where we're going to go, and then I'll bring you up to what's happening today and what's going on in the real world. There is a really exciting area of information technology happening right now in the Defense Information Systems Agency (DISA), which I've had the honor of heading now for the last 19 months or so. It has a lot of things going on. Some of you may have heard of it, some may not, but after today I hope you have a better appreciation of it. I brought a lot of slides on purpose to expose you to everything I think you might ever want to know in your life about this. When I finish, pick out the one or two things that you want to ask me a question about, and I'll answer the questions. I have found that these sessions get better as you ask questions, rather than my giving a presentation. My presentation is one of the things that should kind of whet your appetite, so get your questions and we'll roll on through them. I like to answer the questions because I usually miss a few key things. You have different backgrounds and that kind of stuff, and that's good. So it gives me an opportunity to kind of fine-tune the message and let you know what's going on.

On my introductory slide, I call all of you "Harvard Fellows." I call you that affectionately because I think you're here to do that kind of work: not just to learn, but also to enjoy the fellowship and the exchange of information and ideas. I'm going to talk about "Information Systems Support to DOD and Beyond," and I'm going to talk about what's different in information systems and support over the last several years. I'm going to talk a little bit about the defense environment. I'm sure you've heard a lot about that in recent weeks and days and months. I'm going to talk about the core mission of my agency—the programs, products and services—and a little bit about 21st century warfighting. Then I'm going to wrap up and let you ask some questions.

I want you to know that I know that you get papers to read ahead on most of the presentations here, and I often wondered if some of the students started nodding off about 30 minutes into my presentation because they know I'm not going to give a test, but this time I'm going to review everything, so in case you nodded off last year, if you were here in a two-year program, you'll get a chance to pick all of it up this time. If you want to be here next year, like one young man I know of, you make

sure that if I see you nodding, I'll know you'll get all the word next time also. So I'll keep coming back to the old stuff and take it forward.

Let me show you what the agenda is here in terms of the defense environment (figure 1). I want to talk about the changing dynamics and the changes in problems, warfighter requirements, and the DISA mission.

You know that technology is changing very, very rapidly (figure 2). I use a couple of reference points so you can keep it in mind. As far as I'm concerned, information technology is changing about every 18 or 24 months. If you do anything, or have any kind of program that's going to require more than that much time to field it or produce it, chances are that whatever you produce is going to be obsolete when you produce it. This is a good reference point. Information pull becomes a very critical thing because of the lack or cost of bandwidth. So what you want to do in dynamics now is have the ability for the warfighters or the users to go with this information sphere and pull the information they need, when they need it, as much as they need, on their basis, and not on some basis that you're going to issue to them in a warfighting environment.

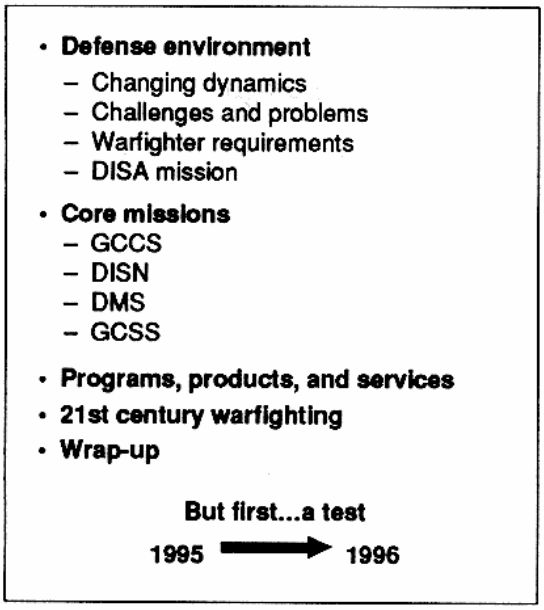



**Figure 1**

**Information Systems Support to DOD and Beyond—Agenda**

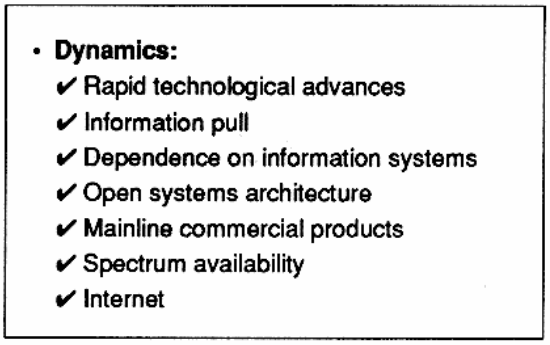



**Figure 2**

**The Changing Environment**

Dependence on information systems is a thing that's happening. Almost every third home now has a computer in it. Almost everybody in this room has a digital watch, and some of the watches you have could even be used as data processing machines. Major Eichenberger has one. He does all kinds of things on his arm right here. So this dependence on information systems is a reality, and we don't have a choice anymore. If you don't sign up to this, you get left behind. It's that kind of an equation now. It's not a question of whether you should get involved in this kind of stuff; it's if you don't, you're going to be left behind.

I won't talk about open systems architecture because people have been using that phrase wrongly for so long they want me to define it for them, and most people who tell you that they're doing open systems are not doing it. So I won't belabor that point.

But this is another key point. Everybody talks about COTS, commercial off-the-shelf products. I don't talk about COTS anymore, because historically in the government we've taken these commercial products and modified them to do the job we want them to do, and once you do that, it's no longer a commercial product. What you really want to do when you take a product—like when you go down to Egghead and buy something—and you want to use that product for 85 percent of your solution, is change the other 15 percent of your procedures to fit that product,

so when the company changes, or goes to the next version of that same product, you can buy it and be compatible. The very day you change one part of it to make it something special, you're no longer working with a commercial product. So I call it "mainline commercial products" rather than COTS, meaning I buy it shrink-wrapped and use it, and when they upgrade or improve theirs (like Microsoft puts out a change on a lot of their stuff every two weeks), if you have a commercial product that's mainlined—that you haven't modified—you can take those changes and stay up to date. That's how I do my systems in my office; I keep up to date all the time. As a matter of fact, Major Eichenberger's almost primary job is to make sure that my mainline products are up to date. He used to teach this stuff at the Air Force Academy, so he should be pretty good at it.

I won't talk much about spectrum availability, other than to say that I'm very concerned, from a warfighter perspective, that we're auctioning off the spectrum, and that one day we're going to wake up and we're going to find that a lot of our systems are operating on a certain part of the spectrum that we've already decided to sell off to make some money to reduce the deficit. We've got some Navy radar systems that you've got to turn off when you come into port, because they interfere with other commercial services around some of the ports. It's very, very difficult. Everybody's happy about auctioning off the spectrum because it raises money, but we have not done a good job articulating to the Congress and to the administration the difficulties with this kind of thing. Also, a lot of the countries in which we are going to deploy will start trying to charge us for this. In the past, we never paid anybody for the spectrum. We just kind of rolled in and did it. Now if you start making billions in the United States, why not do it in another country where we're going to be going?

Of course, the Internet is both a positive and a negative thing. It's a positive thing in that it allows us to communicate very, very rapidly and very, very well. But also, there are a lot of negative things about it. There's a lack of basic security. There are some privacy concerns. There are some concerns about assured delivery of message traffic. You assume that as soon as you've finished typing "SEND," somebody has it, and sometimes they never get it. You're left high and dry. So, while everybody would like just to accept this as the only thing of the future, you must be very cautious about how far you jump on the bandwagon without understanding the vulnerabilities. I thought this morning as I was coming up here about how much connectivity I really want in my own house, and I haven't decided quite yet if I want any. One must be concerned about the vulnerabilities of this. I can tell you some stories about some of the activities that are going on right now in information warfare, some real vulnerabilities, one of which I must say came through Harvard.

**Oettinger:** Hey, you know, you've got to take the good with the bad. We've got Presidents, we've got Unabombers, ...

**Edmonds:** I always show this slide (figure 3) because I want to make sure everybody knows that I won't pick on any community when I talk about interoperability. These are stovepipes. I talked about the fact that this is all hot air that we put out. Every one of these stovepipes has a binmaster (owner) associated with it, and those binmasters think that they're the ones who should run this, and they don't want any interference with you techies or you eggheads: "I run my personnel, I run my intel." The guys who are functional people, who have a Commodore 64, and could do dBase II kind of programming, think they're experts. "Don't bother me with this stuff." If you find guys or gals who are in operations or in plans and policy who also can turn a computer on, they really are hard to deal with because they don't want anybody to help them. So what you have here are custom-built stovepipes on top of stovepipes on top of stovepipes. Even the stovepipes inside the stovepipes don't work together. The day you could get an Army, a Navy, an Air Force, and a Marine Corps logistics system to work together, I will put a medal on you. Even inside the services themselves—the Air Force, the Army, or the Navy—they don't work together. Army

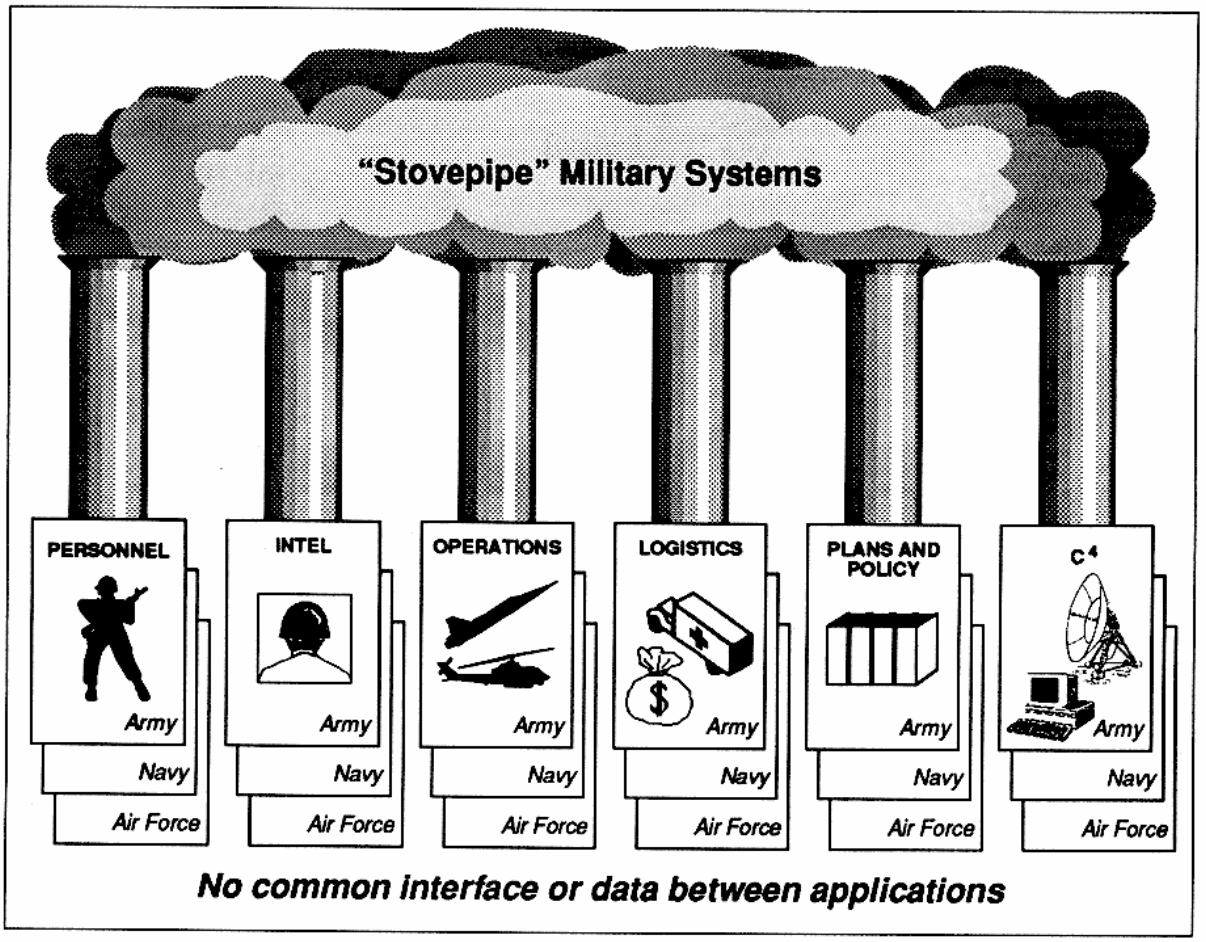



**Figure 3**

**The Problem: Non-Interoperable Systems**

Materiel Command stuff won't work with the Army Training and Doctrine Command (TRADOC). The Air Force Materiel Command won't work with the Air Force's other commands. We have no common data interface, but we're working on it. This is kind of like a problem in interoperability.

It's the same for combat support systems (figure 4). Now if you notice, some of these things show a title like "logistics." I'll talk about that in a few minutes. When we first started looking at command and control systems, we didn't look at these things because they were just too hard. Frankly, I have a bias. My bias was toward C4I for the Warrior (C4IFTW); others' bias was towards combat arms. Once we looked around, we said, "Hey, you really have to do engineering and hire people; you have to buy stuff; of course, you have to have spare parts and transportation; you have to pay people; and you have to keep people healthy." So that's the second part I'll talk about later on in terms of support systems. We call them combat support systems.

I'll just say one word about this slide (figure 5), and that is, we're not very interested anymore, believe it or not, in the left-hand part of the slide—the services—even though it's very difficult to convince the services of this. This is where Title X—organize, train, and equip, which the services have responsibility for—and the real world, in terms of Goldwater-Nichols and where we'll be trying to go, are in direct conflict. We still have light blue, dark blue, green, and brown kinds of systems that the services and the four-star generals, admirals,

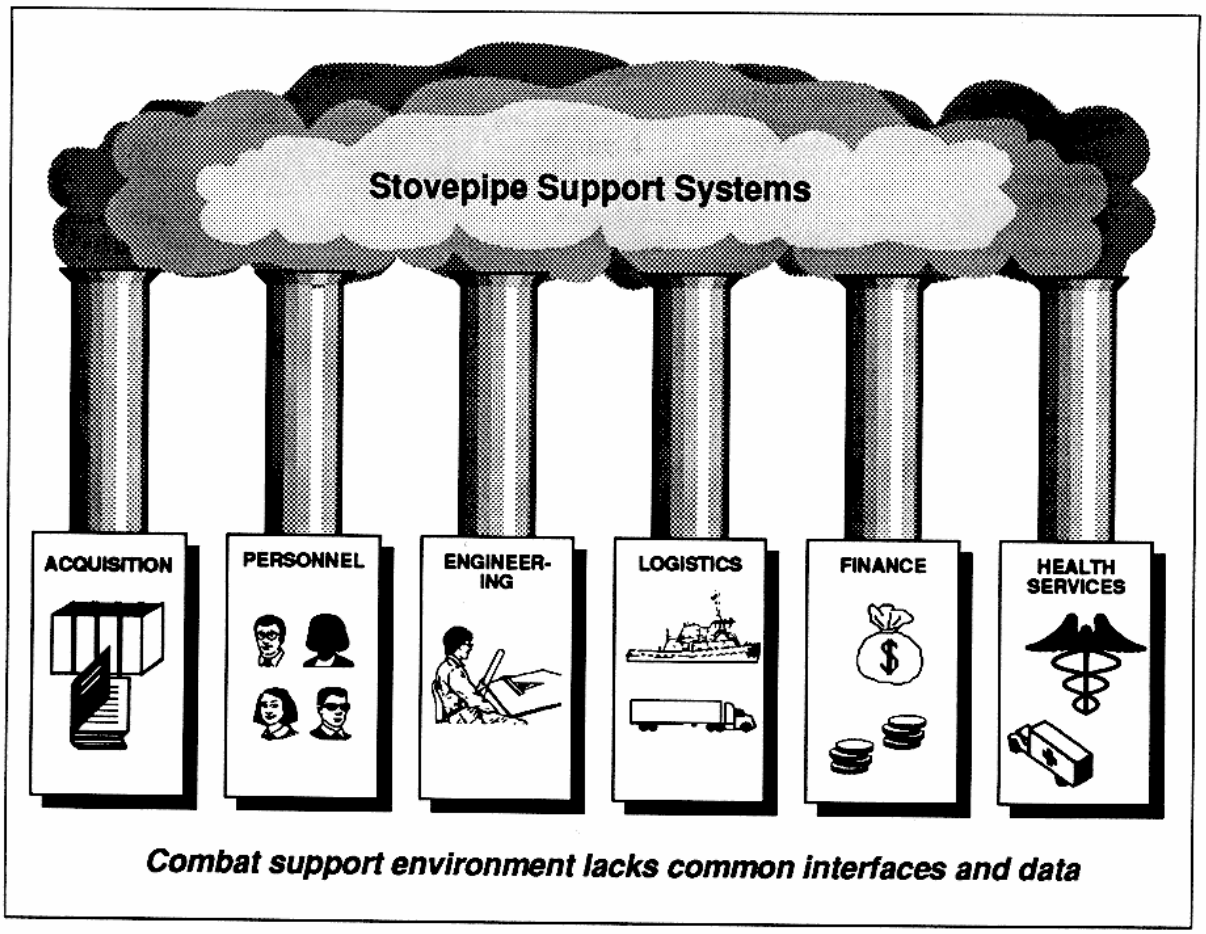



**Figure 4**

**Combat Support Systems**

and secretaries all fight for these programs over on the left side of the slide. They have very limited utility in dealing with our coalition partners, our allies, our joint warfare. As a matter of fact, we have less interoperability sometimes vertically than we have between the U.S. Navy and the navies of these other countries.

As a matter of fact, I can tell you unequivocally that the U.S. Navy and these countries have a system called JMCIS (Joint Maritime Command Information System) that they use right now, and it's the same system. I'm catching a lot of crap trying to get the services to buy this system this way with other things on it called GCCS (Global Command and Control System). That just shows you how difficult this problem really is. Meanwhile, the coalition guys are standing in line wanting to buy it from us so they can get on board. I had the Canadians and some other countries down yesterday asking for these capabilities. So jointness is happening, but we still have these kinds of theological problems among the services.

Now let's talk about the warfighter requirements—the core mission. When I got to DISA, I had to make sure everybody understood that support to the warfighter is the number-one priority (figure 6). Before I got there, people talked about businesses and fee for services and tell me what you want and here's the beer first—that kind of stuff. I'll tell you this: we changed our culture. To prove my point, I'll tell you later on about our efforts in Bosnia and one of the things we did. But I'll focus here on the CINCs. On this slide you'll see no services slice at all. Although we support the services, our focus is on the warfighters.

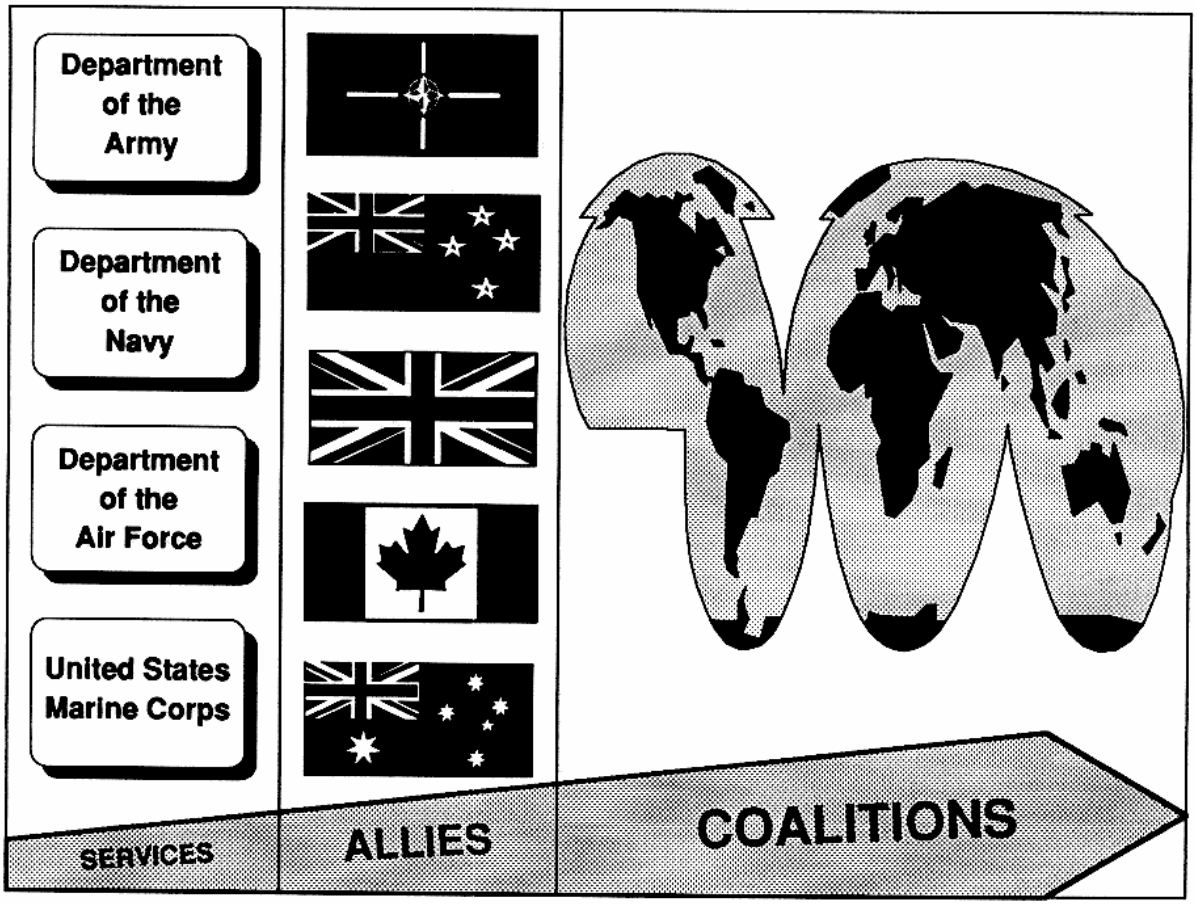



**Figure 5**

**The Challenge: Increasing "Jointness"**

- United States Space Command
- United States Transportation Command
- United States Atlantic Command
- United States European Command
- United States Central Command
- United States Special Operations Command
- United States Strategic Command
- United States Pacific Command
- United States Southern Command

**Figure 6**

**Support to the Warfighter Is Job One!**

This is important (figure 7). If you're going to try to change the paradigms, and to change the attitude of the organization, you've got to make sure you've got some guiding principles. Before I went to DISA, I was J-6 in the Joint Staff, and I had to write the defense guidance that talked about what we should be doing in the Defense Information Systems Agency. So it's easy to go back through it. We called for robust systems, C4I for the Warrior as a vision and the Global Command and Control System as the implementation of that vision, the Defense Messaging System, protection of the Defense Information Infrastructure, aggressive pursuit of enhancement to systems, and the joint warfighter capability. That is what we put in the defense guidance, and the Secretary of Defense supported that. I'll talk about each of these a little bit later.

I show this slide (figure 8) every place I brief. I don't care what the subject is. If I go to church, I talk about this. This is actually critical. As a matter of fact, I even

**Highlights for DISA**

- **Calls for robust C4I systems**
- **Endorses the C4IFTW vision and the GCCS**
- **Supports the DMS and improvements to DOD-wide communications**
- **Mandates the protection of the Defense Information Infrastructure against information warfare**
- **Encourages aggressive pursuit of enhancements to information and communications systems and reductions to infrastructure costs**

***Joint warfighting capability with the ability to reach back to efficient, integrated combat support systems.***

**Figure 7**

**Defense Planning Guidance: Highlights for DISA**

**What the warrior needs:**

**The warrior needs a fused, real-time, true picture of the battlespace and the ability to order, respond and coordinate vertically and horizontally to prosecute the mission in that battlespace.**

***The Defense Information Infrastructure (DII) is the warfighter's highway to the battlespace.***

**Figure 8**

**The Need: C4I for the Warrior**

take the time to talk about your own home. If you talk about this fused, real-time, true picture of your battlespace, think about your house. Think about that you have a car, and the make of that car. Think about that you have to do taxes. You have income taxes. You have a bank account. The grass needs cutting. Your kids have classes in school and they get grades. Your wife has a job. She has a schedule. You've got to take a vacation. All that is your fused picture of your battlespace called your home. It does not make any difference, even at the schoolhouse right here. This course, these things you bring up, are a battlespace. If you don't have a picture of that battlespace, then you don't have the ability to make decisions. You must have a fused picture of the battlespace, and I consider that every day. I have three daughters, I have three sons-in-law, a grandson, a wife, I have 10 brothers and sisters, and that's my battlespace. When my mom and dad left my battlespace, it became a little bit different. Then when my grandson came, I added him to my battlespace. I've been to Florida twice to see him, and so I have to consider my travel costs and take my money down. I have to command and control.

All this is your battlespace, and it's no different for warfighting, whether you're in a cockpit or in a tank, or whether you're downtown in Boston, Massachusetts. You've got a battlespace in your car, sitting behind that wheel, and when that cabbie cuts in front of you, you'd better be able to be defensive. Sometimes you have to go on the offense because he's not going to move, so you swing around him. So this is a very important part of it, and it's not as complex as people try to make it appear. You get things like sensor-to-shooter, C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance). You have all kinds of terms, but you're talking about a fused picture of your battlespace, a ground-truth picture, so you can make a decision, both horizontally and vertically. That's very important. You need information to do that. Dick Macke started this term, "C4I for the Warrior," when he was J-6. The only thing I would change here, if I were to do it over again, is to make the "I" "information" instead of "intelligence," because intelligence is information. There are all kinds of information. So the word would be "information," and then we wouldn't have to be worried about how much intelligence we have in here.

Here's the DISA mission (figure 9). I don't make a whole lot out of it, other than that you should notice the term DII, Defense Information Infrastructure, on the previous slide, because this infrastructure is

**DISA is central manager of the Defense Information Infrastructure (DII) and is responsible for planning, developing, and supporting command, control, communications, computers and intelligence ($C^4I$) for the National Command Authorities under all conditions of peace and war.**

DOD Directive 5105.19
25 June 1991

**Figure 9**

**DISA's Mission**

responsible for planning, developing, and supporting all those things—the command, control, computers, and intelligence for the National Command Authorities under all conditions, war and peace, from the foxhole to the White House.

This is what it looks like (figure 10): intel, ops, logistics, all in a common operating environment (COE). We're going to talk about this common operating environment for a few minutes, and why this is so important. It's important because you want to be able to pull information from all these things at the bottom of the picture on one terminal, wherever it may be. You plug in anytime, anywhere, and pull the information you need, and you don't need to have five, six, seven or eight terminals on your desk.

That's the goal (figure 11). You have to have an objective. To put it another way, you want a common operational picture—smart push, warrior pull. You want to have collaborative planning so you don't have to do a lot of deliberate planning. WWMCCS (Worldwide Military Command and Control System) was doing it for a long time. But the WWMCCS plan was 45 or more days old. You want global interoperability. You want to be able to plug in any time for any mission, any place.

Every time people got to terms and tried to find a way to define the DII, problems occurred. We (our definition) came up with "A seamless web of communications networks—computers, software, databases, applications, and other capabilities" to meet this need (figure 12). That's important because, as you're going to see as I go through this, we are wrapping this world around with fiber, satellites, and everything

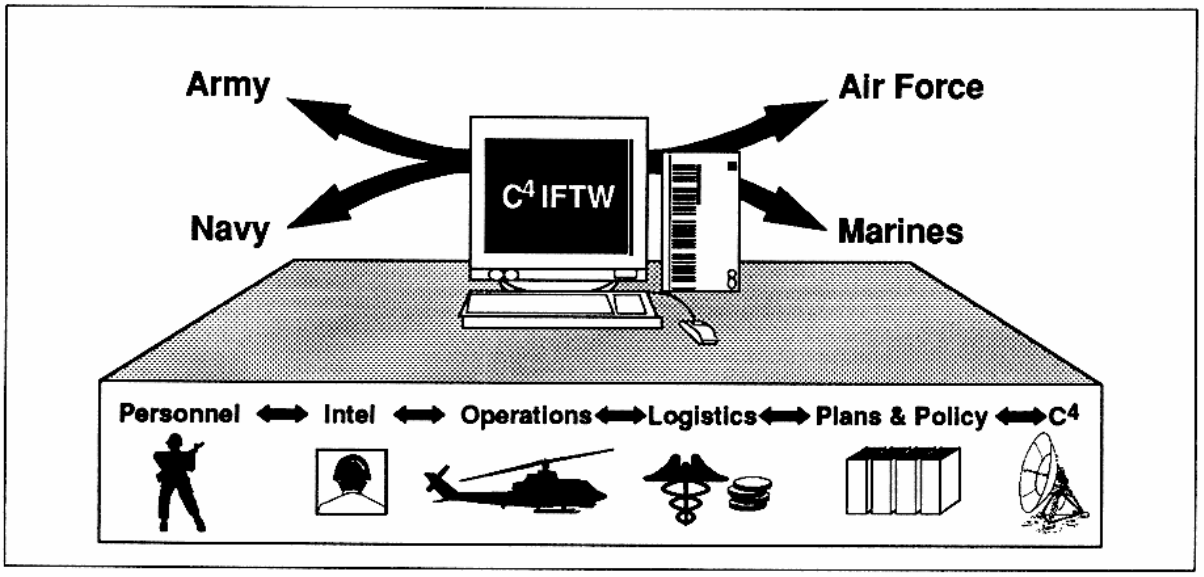



**Figure 10**

**The Objective: COE-Based Systems**

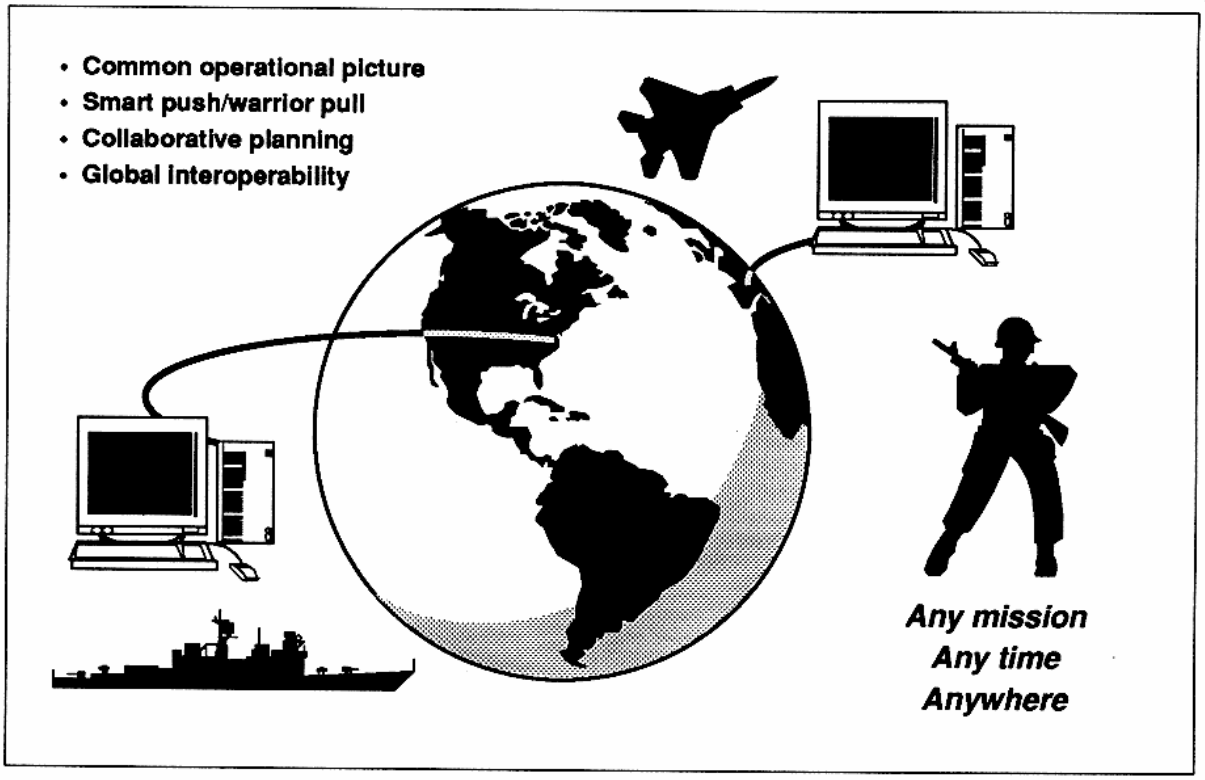



**Figure 11**

**The Goal: Fused Warrior Domain**

we can find to give us that seamless web of systems.

Now I get to core missions (figure 13). Every time I come here I try to come up with something fresh to give the schoolhouse to get the same message across, because this is a continuous message. Nobody ever expected me to go from the Air Staff as a senior communicator to the Joint Staff as a J-6, eventually, and then to DISA, and keep all these themes going for the number of years I've done this. But this is the first time I can remember, in my lifetime and my military career, that we have a possibility of making these things happen before they go away.

I made C4I for the Warrior the top of the house. Forget about the cross-functional, cross-service integration, because that's my job. The other requirements down on the left side and all the stuff on the bottom, some of which I'll talk about, are the things that my agency is responsible for and are about opening the door. We get paid to do things like INFOSEC, and we have the ability to issue some codes and permits, do some modeling simulations, data elements and those kinds of things. That's our job. But these four pieces, the pillars, are the command and control piece, a transmission piece, a messaging piece, and combat support. In the next few slides I want to weave for you an integration of all those things to create the DII.

What you're going to see here is that all the other three pieces need this DISN (Defense Information Systems Network), which is the transmission piece, just to be successful, just to haul information around. DMS (Defense Messaging System) is the messaging piece, and the GCCS and GCSS (Global Combat Support System) pieces need the messaging piece. Of course, they also need a common operating environment, and I usually have a COE sitting right here. But you'll notice in the upper right

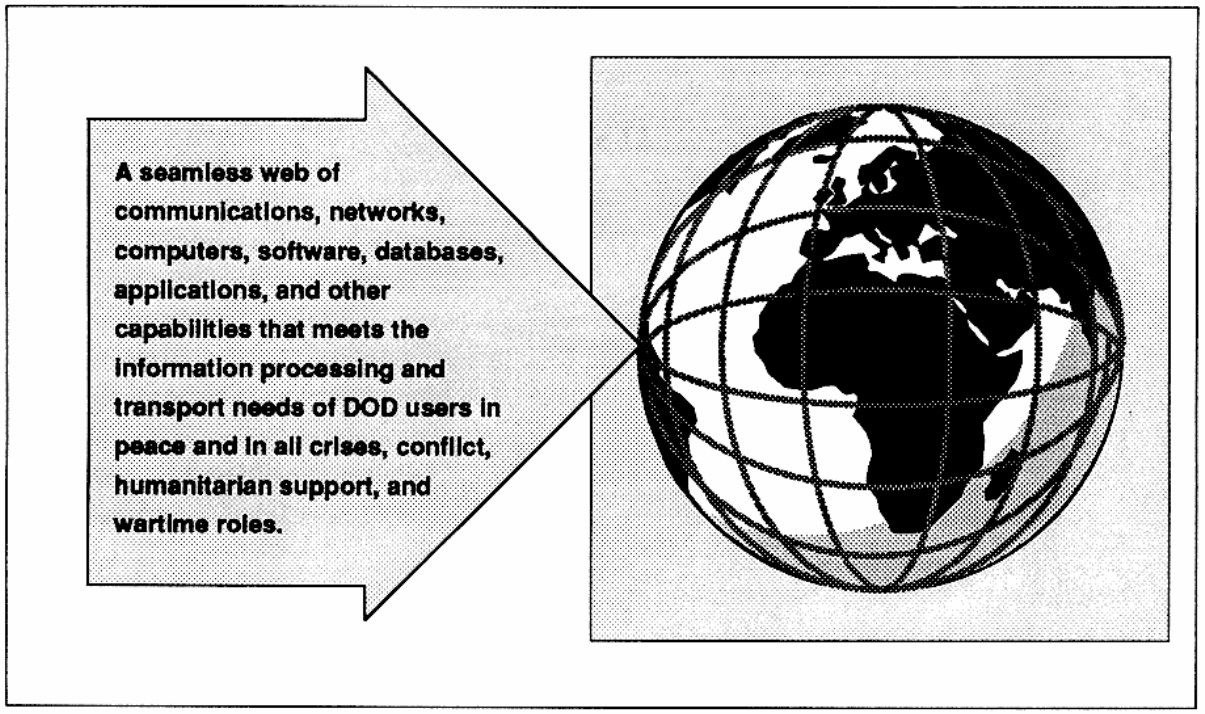



**Figure 12**

**The Defense Information Infrastructure (DII)**

corner that you've got a GII (global information infrastructure) and NII (national information infrastructure), but we're talking about this DII. The bases, posts, camps, and stations in the services are calling on something called BII (base information infrastructure), which is a local infrastructure to hook into this kind of system. But this architectural design is what we're trying to do. I'll give you the status of all four of these things quickly and then we'll get to some other items.

The Global Command and Control System (figure 14) is the operational piece of what I was talking about earlier—crisis planning, force deployment, and force employment—and this is the part I was biased about. At first, that's all I worked for a long time, because that was important to me. This is a significant improvement because what this system really does is give you a fused picture of the battlespace. As a matter of fact, doing Haiti (figure 15), we could see those 60 airplanes taking off from Pope Air Force Base going to Haiti right in my office on my GCCS terminal. The President, the Secretary of Defense, and the Chairman could see the same thing at the NMCC (National Military Command Center). The commander on the *Mount Whitney*, who was an Army two-star, could see the same thing. Two weeks ago, when the Chinese were firing off those missiles in the Strait of Taiwan, we could see the missile event on the same terminal 70 seconds after one was launched. A fused picture of the battlespace—it's here, it's now.

On this slide (figure 15), I have to give credit for this part (ground environment in arrow) to a two-star general named Joe Rigby, who is doing Force 21 for the Army, except that when Joe brought this and briefed me at the request of the Army Chief of Staff, he only had ground environment highlighted, and this was his battlespace. I introduced Joe to a couple of other phenomena called water, air, and space, because Joe thought the battlespace really was the ground. I said, "Joe, you're going to have some guns out here with about 17" jobbies and some TLAMs (tactical land attack missiles) and a few other things, and AWACS, and fighters, and that kind of stuff." So Joe understands

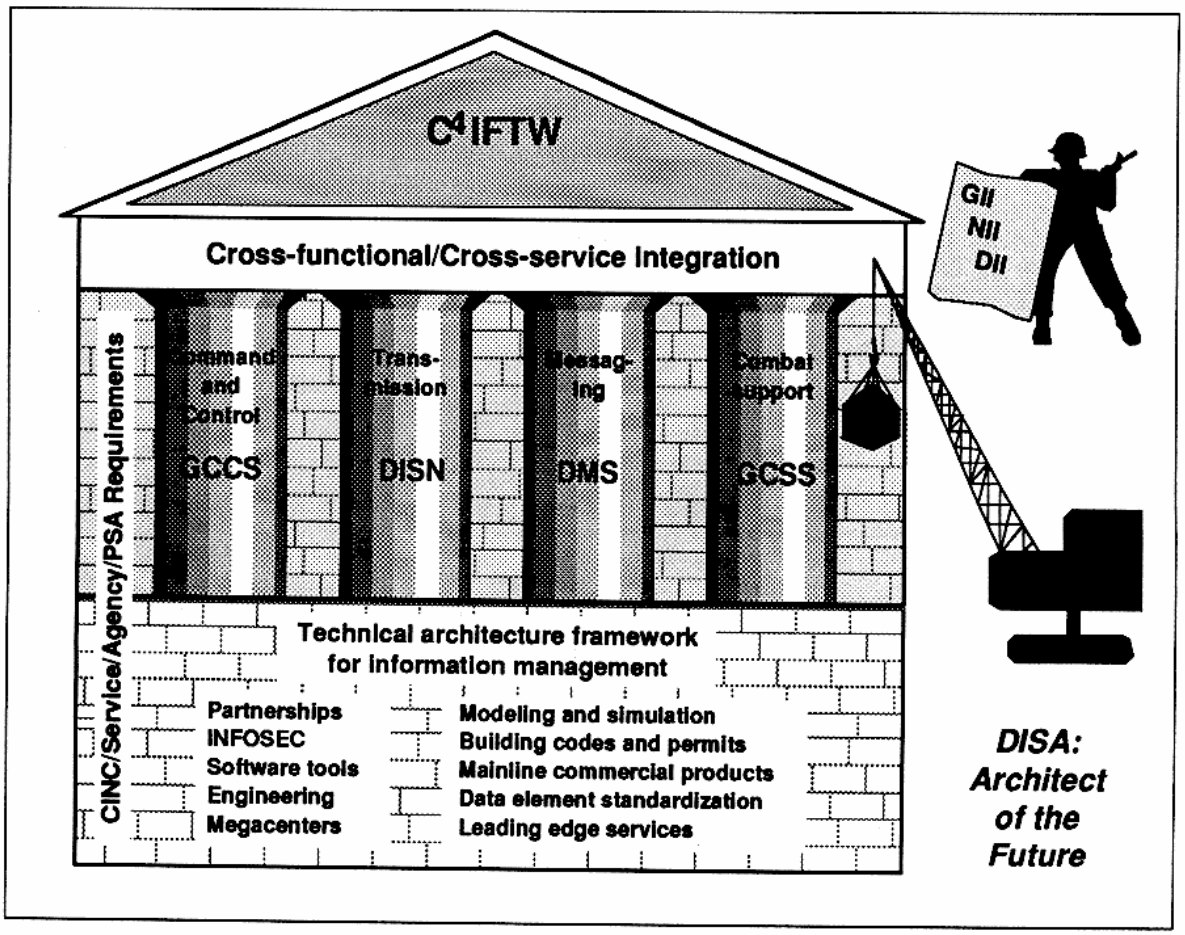



**Figure 13**

**DISA Core Missions**

that. This is real. We could show you this battlespace. There are some warts that need to be removed, but we've used this system already to put command and control at the warrior's fingertips.

Let me just give you a brief objective base (figure 16). When I first came up here, we talked about JUDI (Joint Universal Data Interpreter) and that we would just use an interpreter to show that systems could work together. Some of you have heard of STACCS (Simplified Tactical Air Command and Control System), or OSS (the Navy's Operations Support System), or JMCIS, or CTAPS (Contingency TAC Automated Planning System), and you've also heard of IS (Information Systems) for the Marine Corps. When we first got into this way back when, with Dick Macke, we put those four systems together. We had some smart guys down at the Patuxent River and we told them to see how much commonality there was between those systems. Seventy percent of those systems were the same, and the data elements were also the same. A lot of them had been developed by the same companies, and we were paying for them four separate times, and never did the four come together. We've graduated from this now, and we have a whole objective phase in this area.

That's command and control. Right now, on April 22, 1996, we're probably going to declare victory on this whole thing, and we're going to turn WWMCCS off. It's been on for 25 years. It cost a lot

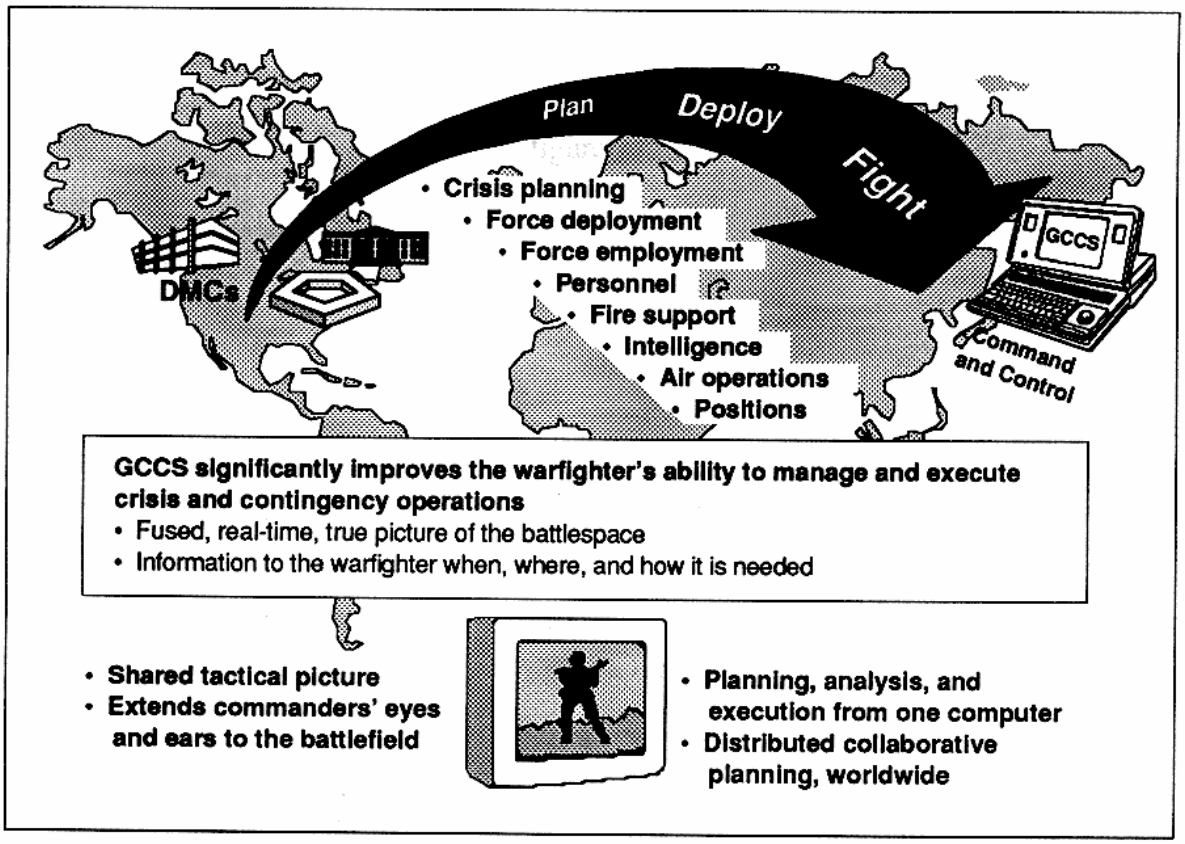



**Figure 14**

**GCCS**

of money. We're going to put three or four of the major warplans in the GCCS on that date, and we're going to put all the other warplans in after that. But this is happening two years from when we started. We broke all the rules of casual acquisition, or whatever people want to call it, because we wouldn't get captured by the MAISRCs (Major Automated Information Systems Review Councils), the DABs (Defense Acquisition Boards) and those kinds of things. We just did it, because the Chairman [of JCS] and the Deputy Secretary of Defense told me just to do it. So we did it.

Now that was the command and control piece. This is the DISN, the transmission piece (figure 17). It's very important to allow the warfighter to plug in and push or pull information. It's going to support multimedia bandwidth rather than just voice-equivalent kinds of circuits. We're going to do bandwidth on demand. That's critical to us, because we never have enough bandwidth.

Here's the status (figure 18). Right now, in the CONUS, part of the contract is out for bid, and we have two of the bids in already. We're going to start working the Pacific and, for the first time since Hawaii became a state, we're going to have some competition out in Hawaii for telecommunications. The Department of Defense is driving it. We're working Europe because almost all of our switches, our systems, in Europe were waiting for the Russians to come through the Fulda Gap, and the systems are old and need replacing. Now we have to do the process of getting commercial capabilities. Then we're going to work to deploy DISN. That's very, very important, but the thing we're trying to evolve to is what I call virtual command and control capabilities, not hard systems.

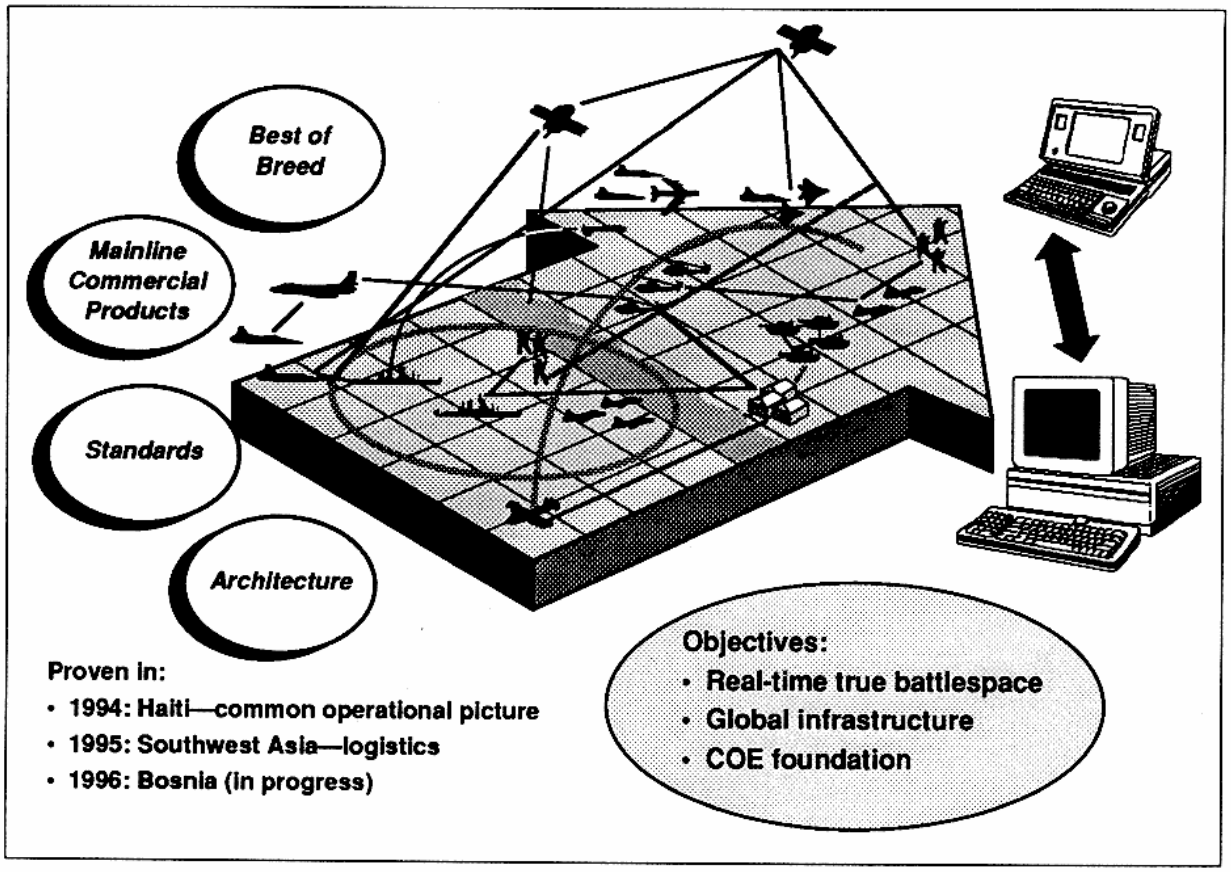



**Figure 15**

**GCCS Approach**

**Student:** Sir, if I could interrupt you: so South and Southwest Asia then are going to get covered by deploying DISN?

**Edmonds:** Yes. As a matter of fact, we're building some infrastructure in Southwest Asia. Almost all of it right now is U.S.-owned because it's of a tactical nature, and we are putting in some infrastructure. For instance, in Bahrain we now have a satellite earth station. We're going to run fiber into Bahrain coming around India, up through the Gulf, but deployed DISN is now going to cover most of it and commercial SATCOM will fill in the gaps.

We still support a lot of Southwestern Asia by reaching back into Europe and to the CONUS. As a matter of fact, almost all of the services now have what they call a reachback concept, where you don't put a lot of structure forward. You just get a big pipe coming back and hit someplace on the East Coast or in Europe, and you get all your comms back that way. DISN is the primary piece. Anyplace where we do not have a real big-time U.S. presence, we're going to deploy DISN.

Almost on my own initiative, I'm buying deployable commercial capabilities to extend the DISN wherever you want it to be extended. We're also into three contracts of wrapping fiber around the world three times, and we're going to pop out in several strategic places around the world so we can plug in there and hit that spot with commercial satellites, fiber, or military satellites, and get you to where you want to go. We call these strategic-tactical interface points. We're doing that right now as a separate project. So what we're going to be able to do is get you to one of nine spots on the face of the earth, then we'll get you to where else you want to go. We're also buying capability on the Iridium satellite,

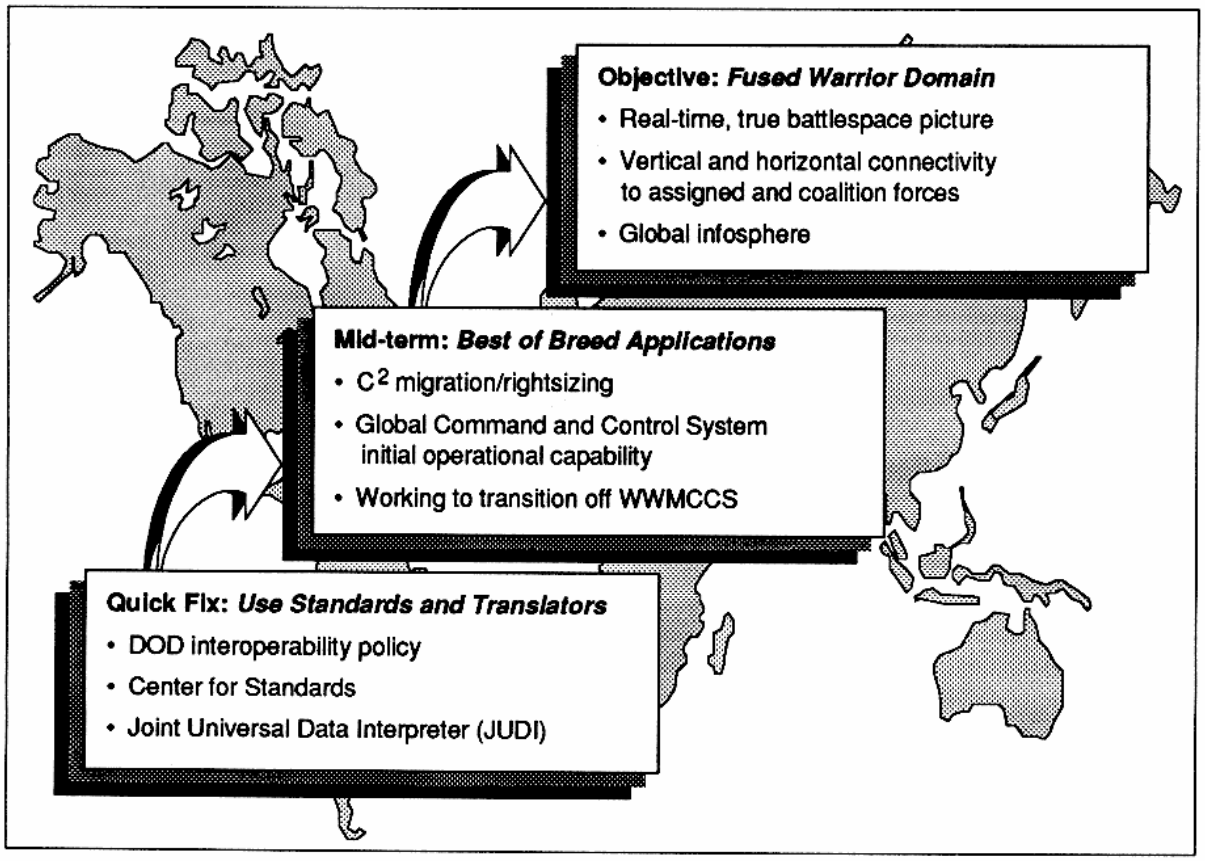



**Figure 16**

**GCCS: The Bridge to the C4IFTW Objective**

the 77-satellite Motorola configuration, so we can plug up and apply those and do the same thing. We're negotiating right now with Loral on Globestar for the same capabilities. So wherever on the face of the earth you want to be, we'll be able to put you right there. I have an option for 45 transponders from COMSAT worldwide. Remember when I talked about the CRAF (civilian reserve air fleet)? When we do airplanes in the Air Force, we pay airlines a little money to keep their airplanes reinforced to haul tanks and troops. So we put a little money down for the transponders in the same way. The only guy that CNN worries about is me, because I've already got these optional 45 transponders, and they think I'm going to get there before they do.

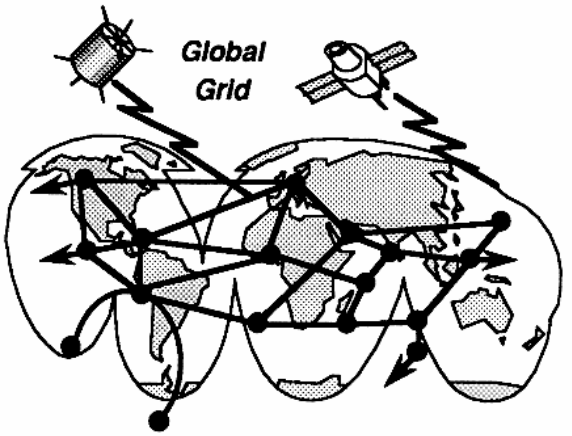
Here's the Defense Message System (figure 19). When I was a second lieutenant, I used to do test and accept for AUTODIN-proprietary formats. We had all kinds of e-mails around the whole county and around our department, and we got dog breakfasts. They were dedicated, and they were cumbersome. Right now, I get about three messages a day on AUTODIN. I get a message from the Air Force telling me where all the generals are going. I get one from the Joint Staff telling me where the Chairman and the SECDEF are going to be traveling. In case my comm breaks, they want to make sure I know where they are. Then I get a third one where they kind of complain about something I've done that they didn't like. I take about 10 seconds to read all three messages, then I put them in the trash. I get about 150 e-mails every day, and that's how I run the agency: with worldwide e-mail and my DISANET.

The old AUTODIN that I did test acceptance for as a second lieutenant is actually costly and labor intensive. There are

**DISN is the DOD's worldwide protected network allowing warfighters to "plug in" and "push or pull" information in a seamless, interoperable, and global battlespace.**

**Supports multimedia, bandwidth**

- Transport system for the DII
- Global, scalable, technology-based




***Switched virtual circuit bandwidth on demand for achieving full integration of voice, video, imagery, and data.***

**Figure 17**

**Defense Information System Network (DISN): Transmission**

15,000 people tied up doing that old work. I went down to one base the other day, and they've already put in two people doing it for the whole base, full time. They just take the message off AUTODIN and put it on a floppy, and put it over here on the LAN. And so, it's going to go away.

Defense messaging is a new thing: multimedia capable, with global addressing, so wherever you are, it will find you, whether you're T. Oettinger, Tony Oettinger, or Oettinger, T., or whatever. We'll also address this writer-to-reader. It's not to an organization, it's to *you*—at home, at the airport, at the office. You will have secure and authenticated messaging. You can use that DISN backbone, and we're also working on our joint/allied formats. So this defense messaging is very important.

Here is the status (figure 20) of the Defense Message System, and these are some features of it. We hope to have our Sensitive/Unclassified IOC (initial/interim operating capability) in July, and we're already trying to do that sooner. We'll have a Secret capability pilot in July 1996, and then we're actually going to do it in 1997.

We have a sundown clause with AUTODIN. It goes away in the year 2000. It will save us $2 billion and 15,000 people. I'm going to beat that date. I'm going to try to make that happen in July of 1998 rather than the year 2000, so we'll save money and people. The technology is moving so fast that we're going to be able to do this anyway.

We want to get to the point where it's shrink-wrapped. Monday of this week [April 1, 1996], Microsoft had a big announcement. Microsoft Exchange is one of our contractors. It's one of the packages we're going to use for messaging in the DMS, and DMS is a big driver for that.

What does a DMS user need (figure 21)? You can take any of these user agents. We have this Fortezza card that I usually bring, but I'm sure I didn't bring today. It's in my laptop computer. I'm going to use the DISN backbone, the global directory, so that anywhere you are you'll find the person you want. A lot of information is going to be on your own computer. We're going to have a certificate authentication workstation that will authenticate that you are, in fact, who you say you are. We'll provide this infrastructure for the whole Department of Defense so that the user does not have to buy any of this. You provide your own desktop. We're kind of debating how many of these Fortezza cards

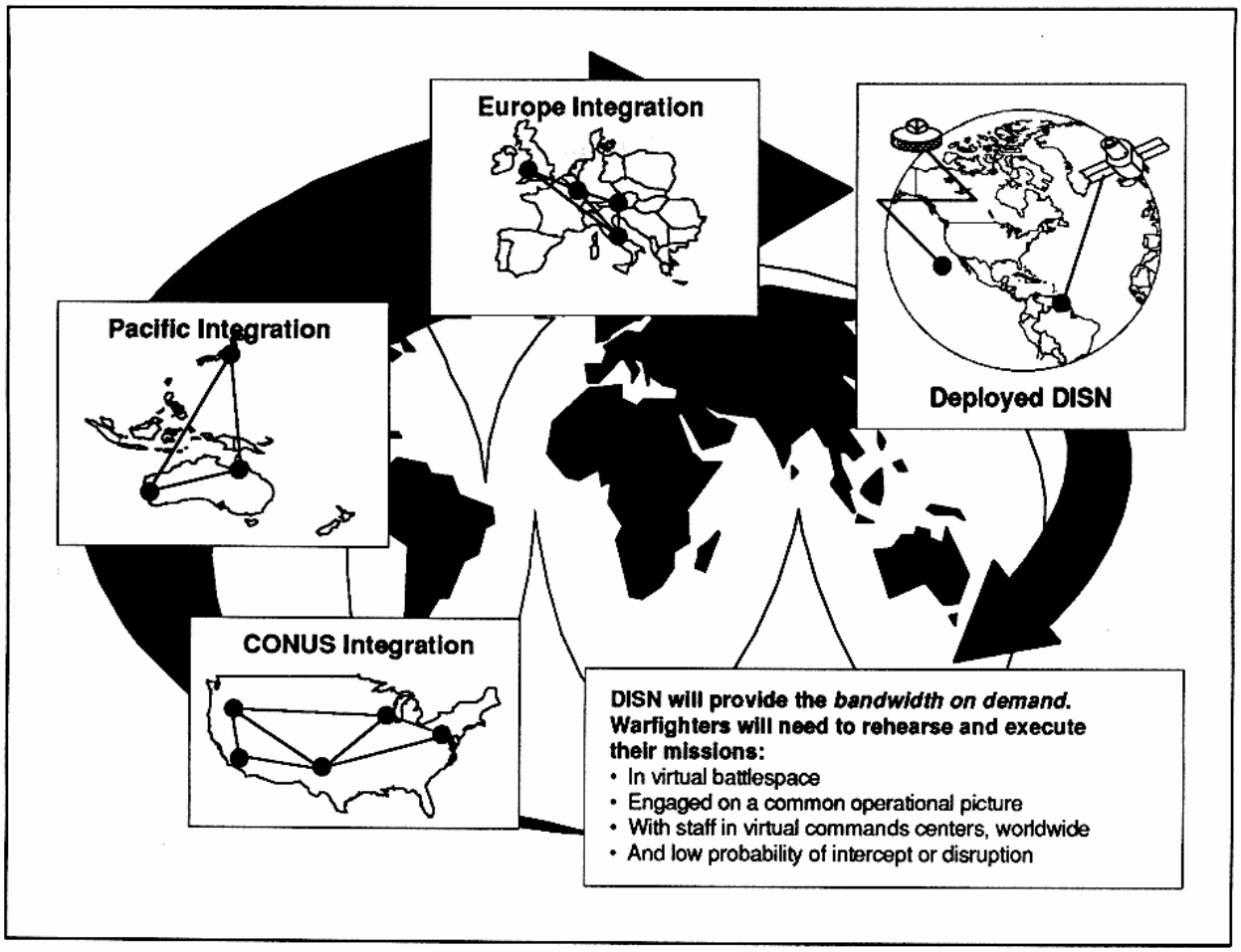


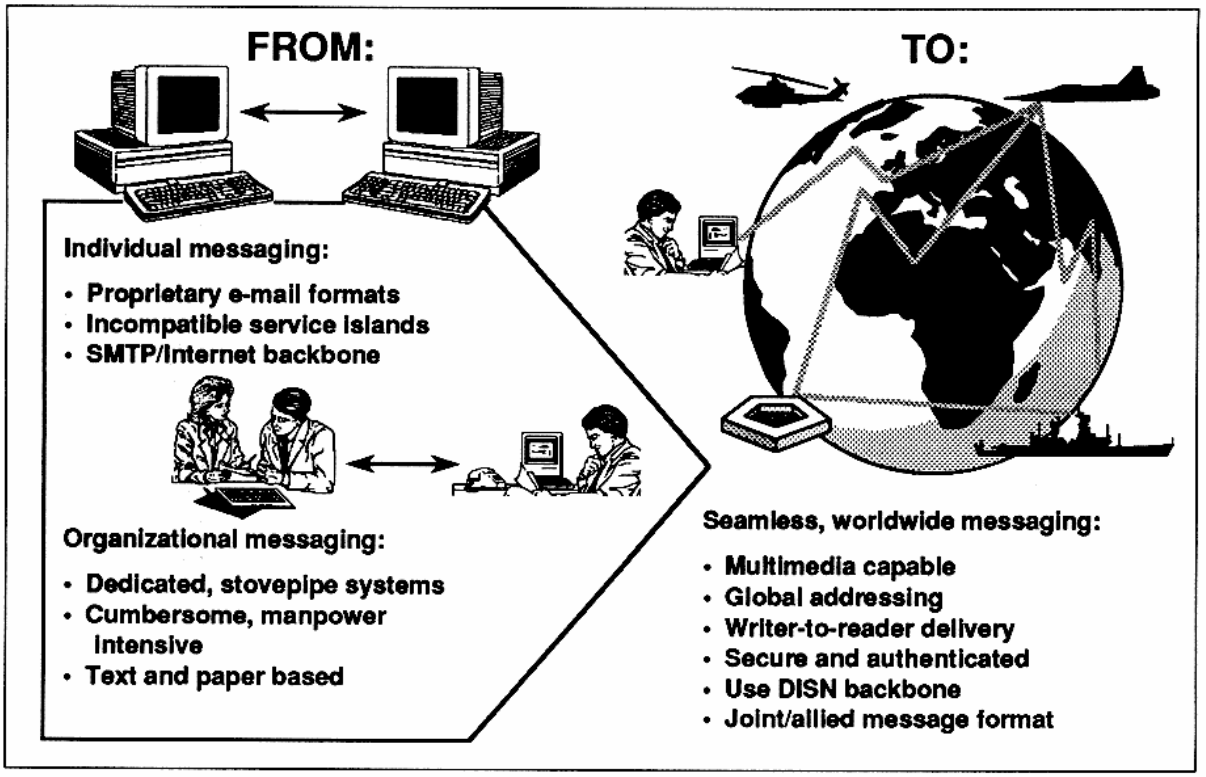

**Figure 18**

**DISN Status**

we have to buy versus the customer buying them. We wanted to buy them all, but the customers (the customers are the Army, Navy, Air Force, and everybody else) said they want to buy their own because they think they can hold out until the last minute to put the money up. But we're going to provide everything but your desktop workstation and make it happen. So we'll be down into the nits and grits here.

Now, I'm going to change the pace a little bit and get to global combat support (figure 22). Remember that I told you I had a bias against the operations stuff? But I found a quotation from Shalikashvili that I could use to get me interested in this combat support thing. When I found this, I said, "Okay, we need to start working this thing we're talking about in UNESCO, this reachback, get support from CONUS, and then use comm pipes.

These are things you saw before (figure 23). Here are the combat support activities. You'll notice I have these arrows going in here because I want to beat this into one thing, called the Global Command and Control System. You'll say, "Well, why are you making things that are so close together—GCSS and GCCS?" We did it on purpose. We don't want a new start. You may remember that this was once the domain of CIM (corporate information management), and we got in trouble with that program because we did not deliver very much. So we kind of cut our losses. We said, "What can we get out of this program and salvage something for the user?" We took all those same functions that we were




SMTP = Simple mail transfer protocol

**Figure 19**

**Defense Message System (DMS)—Messaging**

**Features:**

- **Worldwide, from White House to foxhole**
- **Joint service, ally and coalition interoperable**
- **Secure end-to end, guaranteed delivery**
- **Shrink wrapped**

**Status:**

| | |
|---|---|
| • Sensitive-unclas IOC | July 1996 |
| • Secret capability (pilot) | July 1996 |
| • Secret IOC | July 1997 |
| • Top Secret IOC | July 1998 |
| • AUTODIN sundown | 2000 |

***DISA is responsible for DMS infrastructure and product compliance testing***

**Figure 20**

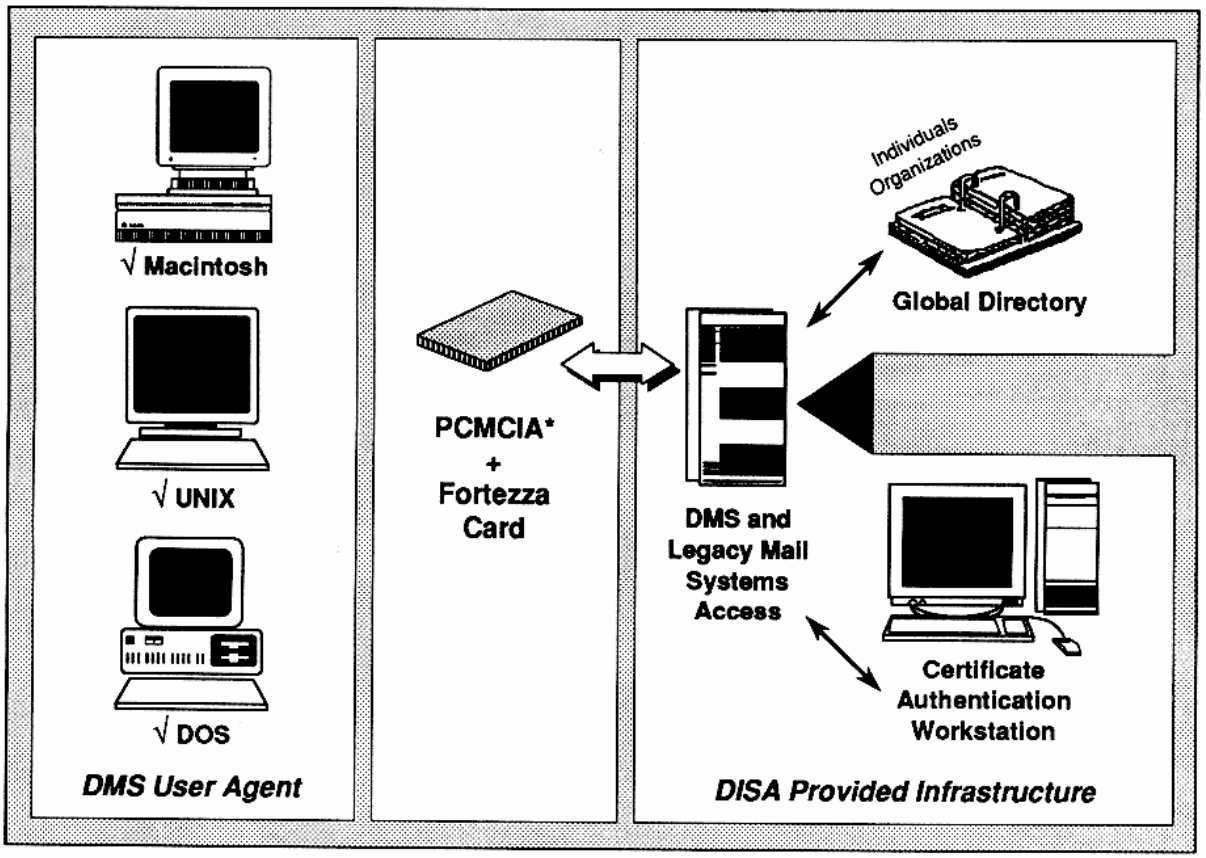
**DMS Status**

trying to do corporate information management for, and we're now going to try to interface some functions first and integrate them later to make this thing a reality for the user.

**Oettinger:** Could you comment either now or later on the reasons for that push? Was it the nature of the administration, the nature of the task, or all of the above, in what proportion, because that might be limited? The height of CIM was earlier, so . . .

**Edmonds:** Yes, I'll mention it right now. When we first started doing corporate information management, I think that Paul Strassmann, Secretary Atwood and Duane Andrews* had a great idea in trying to get

* Paul Strassmann, Director of Defense Information in the Office of the ASDC$^3$I, 1989–1992; David Atwood, Deputy Secretary of Defense, 1989–1992; Duane Andrews, ASDC$^3$I, 1989–1992.




*PCMCIA = Personal Computer Memory Card Industry Association

**Figure 21**

**What Does a DMS User Need?**

rid of all those legacy systems and migrate to some common system so we could save money and get rid of a lot of people who were around, and the amount saved was in the billions of dollars. It was a good idea. I had an interview with Paul about a month ago, and he said, "We made one mistake. We miscalculated. We thought we were going to be around for seven years, but we were around for three years. When that administration went away, and a new administration came in, they never did really understand what the endgame was supposed to be for CIM, and so they were kind of lukewarm toward everything in CIM. They tolerated it and kind of let it go along because Congress accepted this as a way to save money in the Defense Department." They also allowed each one of these bin-masters (system owners) here to kind of run the whole show, and that was a mistake. Each one of these guys in charge of these things in OSD is an Under Secretary or Assistant Secretary. They're all political appointees. You'd think that the Secretary of Defense and the Deputy Secretary could tell them what to do. They can to a point, but most of these guys have a personal relationship with the President or the Vice President, or some big wheel someplace, and if they don't want to do anything, they won't get engaged in it. I've watched that happen. They don't want to deal with it. You say, "I want to take over your system and make something out of it." They say, "Sure." If I go tell Dr. Hamre in finance that I want to take his DFAS (Defense Finance and Accounting Service) and do something else, he will say, "I don't do that," or if I tell Dr. Dorn that I want to do something with his personnel stuff, if the lady who works for him doesn't tell him,

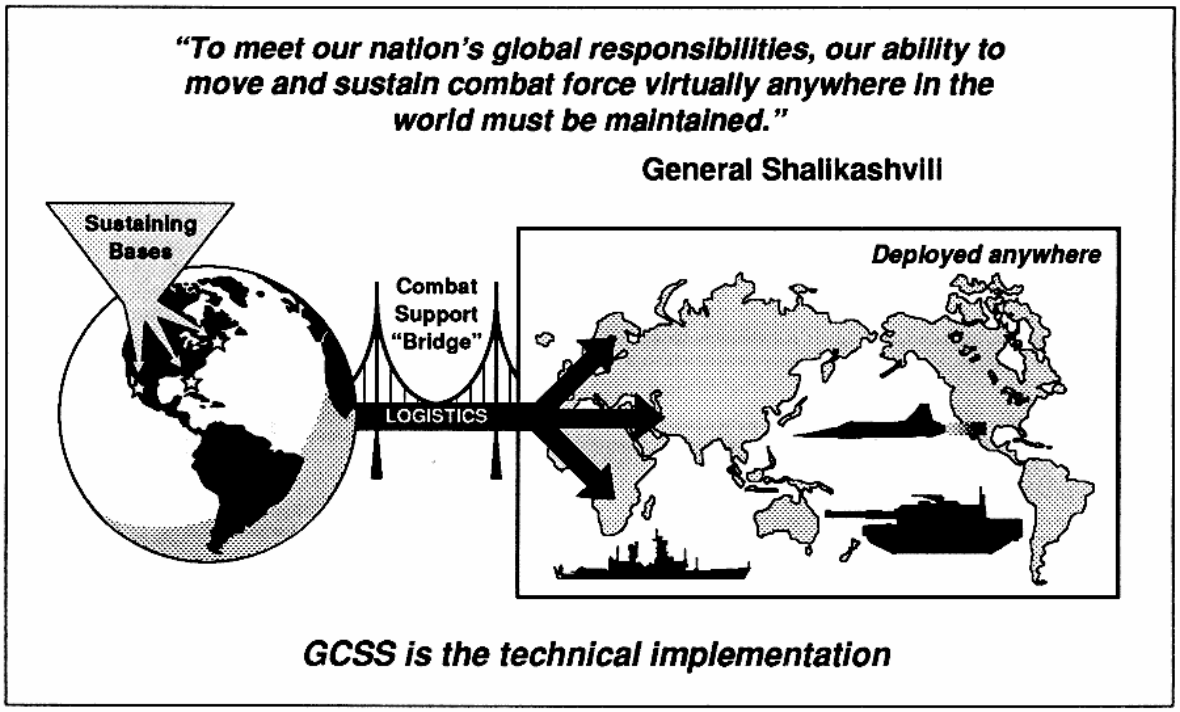



**Figure 22**

**Global Combat Support System (GCSS)—Combat Support**

"Yes," he wouldn't say, "Yes."* As a matter of fact, if you asked him a question, he would look at her and she would give him a nod, and he would say, "Okay." So that's too hard.

The other thing is that the services were left with the legacy systems and a mission to do somewhere, and the moneys were taken away from them. So they're not interested in giving up any more money, or in getting your assistance. It really was a bankrupt approach, so we had to think up business process reengineering. You've read all this in your books: "We're going to reengineer government, reengineer all these things, and we're going to do it right, do it differently." We spent hundreds of millions of dollars getting the process right. Well, you could spend all the money you want to, but if that guy over in the Air Force says, "I'm not going to do that," I don't care what you say; it's not going to happen.

Let me tell you why. We get down to real basic things: to trying to make the services do something. The secretaries of the services and the service chiefs say, "I'm a Title X. I'm responsible for organizing, training, and equipping, and this is, in my estimation, organizing, training, and equipping. See you guys later." So they start burrowing down, hiding their money, and doing all kinds of things, and most of the systems are still around, and most of the interoperability problems are still there. And so, there are two things we've done now to change things. You no longer get CIM money to do any of that business process reengineering unless you bring matching funds. So if you want $10 million, you bring $10 million, and you have to tell us that your $10 million that you're going to spend, plus our $10 million, which is $20 million, is going to help you become compliant with this common operating environment of the GCSS. We now have them signed up for this. It's a way to get people to build to this common operating environment rather than trying to dictate to folks what system to have or not to have.

* John J. Hamre, DOD Comptroller; Edwin Dorn, USD for Personnel and Readiness; Diane Disney, Deputy ASD, Civilian Personnel Policy.

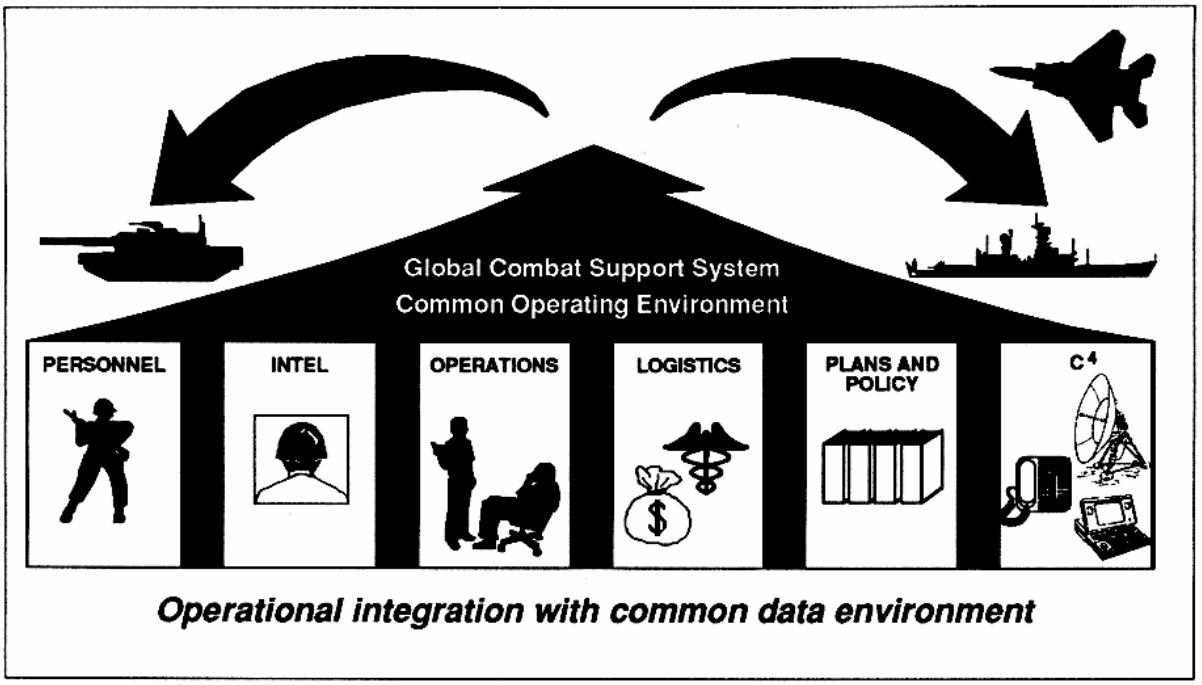



**Figure 23**

**Global Combat Support System**

We'll just put this common operating environment out there and say, "To be compliant, and be able to use this, this, and this, you have to build to this. It's a new system, so migrate the old system, that's what you do." That was our strategy. We made a conscious decision last summer to do that. So now, you bring matching funds, or you don't get any CIM central funds at all. All the other CIM dollars that we had are now rolled into the GCSS.

**Oettinger:** Is the carrot working?

**Edmonds:** Oh, yes, it's working. As a matter of fact, I would say that later this year, you probably won't see any more RFPs or any procurement on the street unless they have this statement in it: that you must include a GCSS COE-compliant system as a deliverable. The MAISRC people have sent us every one of the RFPs now for review to make sure they have the right provisions to ensure that when they finish, they're going to be compliant with this common operating environment. This is tough on some of the services' acquisition houses, because they've been free-wheeling for so long, and now they've got to have some discipline. I have the money, and if they want to get any support or any help from us, they have to comply with this. That was a conscious decision made by the Deputy Secretary of Defense, because nobody else had any other fresh ideas on what to do about CIM. Otherwise we would continue to go forever and ever.

**Oettinger:** Am I hearing you correctly? That seems new. In the old days, the Defense Communications Agency and then DISA was kind of a contractor that sucked up money from potential clients. You're now saying that you are the dispenser of funds?

**Edmonds:** Exactly. For instance, the Army is the lead military department for DTAV (Defense Total Asset Visibility); the Deputy Chief of Staff for Logistics is the OPR (office of primary responsibility) for it. To do his job, he needs support from me, and I provide funding to him in addition to other funding that the functional guys give him to do his job. The Air Force, out at United States Transportation

Command, are working in-transit visibility. They call it OCIMT, the Office of Corporate Information Management and Transportation. I have provided both people and dollars to help them be successful in building to this common operating environment. For the telemedicine guys, we're working to make sure that their applications, their systems, are being built for it. I contribute both people, in small numbers (five to eight), and money. I pay their salaries out of the CIM central fund, and I provide money to them to help them with their contractors to make their systems COE-compliant. They must show and prove to my engineers that they're on a path for this kind of compliance, or they get no money.

If they're fortunate enough to have a system that a DOD community, like intel or personnel, has rallied around as the system they're going to migrate to, then we can give them more support. We can take that system and together we can clean it up, fix it up, and put it on the migration path so that this thing that has become their system of choice can become a GCSS-compliant system that everybody should build toward or interface with. We have those dollars in my budget to do this job.

Now, remember I told you that I had to buy some command and control, and I hated this at first, but now you see what we have here (figure 24). We sold this to the Secretary of Defense: that we tried to take the operational part, which is plan, deploy, and fight, and includes crisis planning and those kinds of things, and put it into command and control, GCCS. Then you will notice that things like reachback, medevac, resupply, finance, and engineering, which are combat support things, I have here in the redeploy and sustain part. That's the GCSS. This is the sum total of combat support and command and control, which together make up what I call the DII, the Defense Information Infrastructure of these functionalities riding over the DISN.

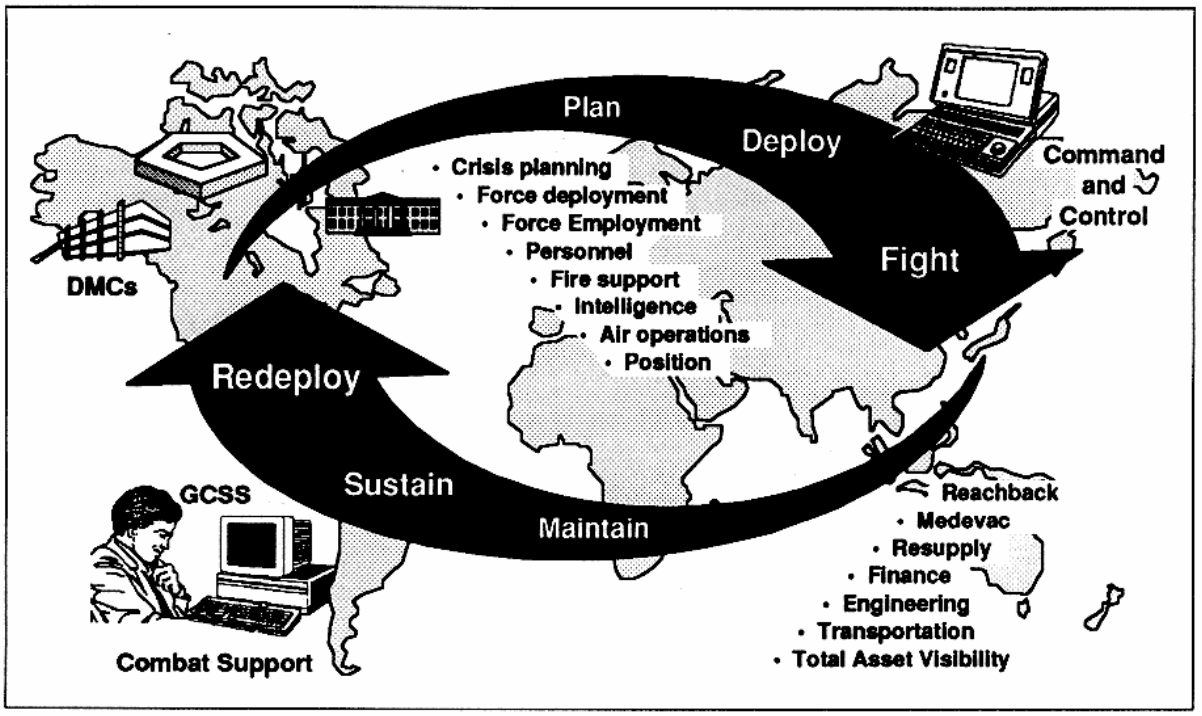
Let me change pace. I'm not going to talk about this a lot (figure 25). I understand you get a lot of this up here in the schoolhouse, but you know these things about information warfare. I won't say much, other than that I'm responsible for building and defending the DII.

I'll just go through these things really fast (figure 26). You know that dial-ups are one of the biggest problems. You also know that the infrastructure is vulnerable. Dialing into the system, you can get to a lot of the rest of the stuff.

You also know how we protect the systems (figure 27). We have some tools. We have some policies and procedures, and do a lot of training. What we try to do in a bottom-line kind of way is get automated vulnerability monitoring tools to go on our systems, rather than manual systems. The one we're actually working right now assumed we put a server on the system. The people who are trying to get into this system didn't know what it was. They stopped for a while, but now they're active again. This is a very big area for us.

Now, let me tell you about programs, products, and services. This is one of the things I want to introduce you to (figure 28). You've probably heard a lot about electronic commerce and electronic data interchange (EC/EDI). I never wanted to be bothered by this in my life, but I got stuck with it. It's how government does business—buy stuff electronically. We buy a lot of things over that old wire. Right now, we provide the network to allow DOD and a lot of the federal government to order things over the electronic wire. We put out an RFP, people can come back over the wire and bid, they're selected, and we purchase the product. There is a lot of competition, it gives us best value, it gets out fast, but it's been a nightmare. It's an absolute mess. But, let me tell you, the President and OMB love this electronic commerce stuff, and right now we're doing about 10,000 or so transactions a day (figure 29). We expect in another four or five years we'll be doing over a million and a half electronic commerce transactions a day. There's one other task that we've got to do with this ordering stuff. Dr. Hamre in finance wants me to automate the paying function to go with the buying. So buying and selling and this kind of stuff is going to become big-time business, and that's part of this combat support.

Right now, we have a terminal, a server, out in Bosnia where the on-the-ground Joint Task Force commander and




DMCs = Defense Mega Centers

**Figure 24**

**$C^2$ and Combat Support**

- **Low cost way of waging war**
- **High payoff option, compared to cost**
- **Without boundaries in time or geography**
- **Low risk to attacker; difficult to determine source**
- **Available to all states, organizations, individuals**
- **Unsophisticated technology to employ**
- **Significant force multiplier**
- **Serious threat to everyone**

***Something we can (must) defend against***

**DISA's Role:**

- **Defend the DII**
- **Assure systems availability**

**Figure 25**

**The New Battleground**

his people can buy commodities through electronic commerce with a comm line from Bosnia back to Columbus, Ohio. He gets right on his network that we're providing, and he can get his stuff the way he can when he's at home—whatever he needs to buy, up to $100,000 kinds of commodities.

This is a good-news story (figure 30), and it also relates to DISN. We have gone out and gotten this commercial satellite initiative to augment our military satellites, and I have that option to have 45 transponders worldwide that I can get whenever I need them. I can put anything I want to put over them. I'll show you in a few minutes how we use them. But I want to take this moment to tell you why that last slide is important.

We've built a model in the Department of Defense to simulate two major regional conflicts (figure 31). We've taken each one of the CINCs' warplans, and we've modeled them based on these two MRCs. Everywhere you see white and black, in a 150-day two-war scenario, DOD does not have enough bandwidth to satisfy the warfighters' requirements. Where you see

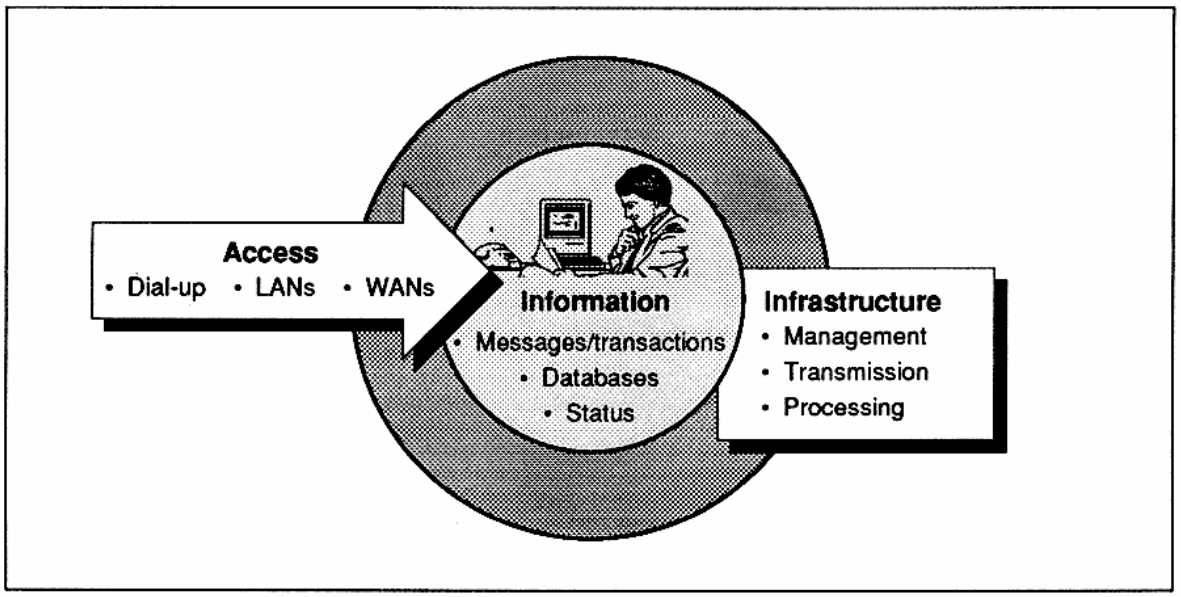



**Figure 26**

**What to Protect**

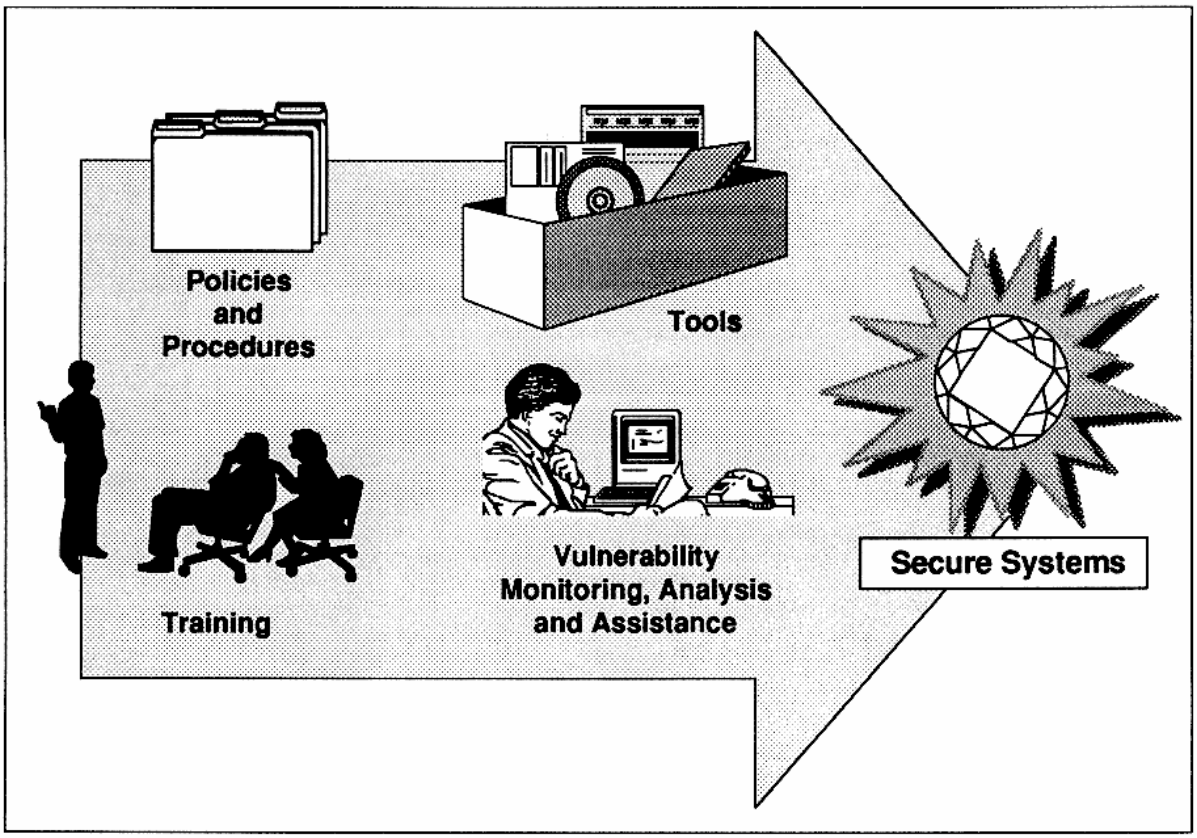
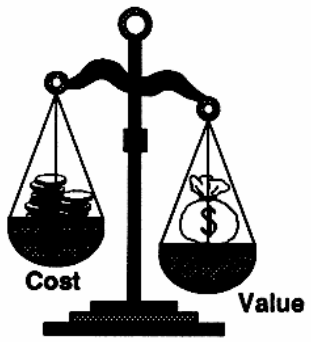



**Figure 27**

**How We Protect**

- **It's here, now!**
- **It's how the government will do business**
- **You need to be a part of it**
- **It fosters competition**
- **It gives us best value**
- **It helps achieve interoperability via adherence to standards**




***It's a win–win situation***

**Figure 28**

**Electronic Commerce/Electronic Data Interchange (EC/EDI)**

**Emerging technologies:**

- Electronic catalogues
- Prime vendors
- Quick response
- Virtual shopping
- Virtual inventory
- Virtual products
- Integrated Standard Procurement System role

**Potential functional areas:**

- Health services
- Medical supply
- Transportation
- Personnel
- Finance...

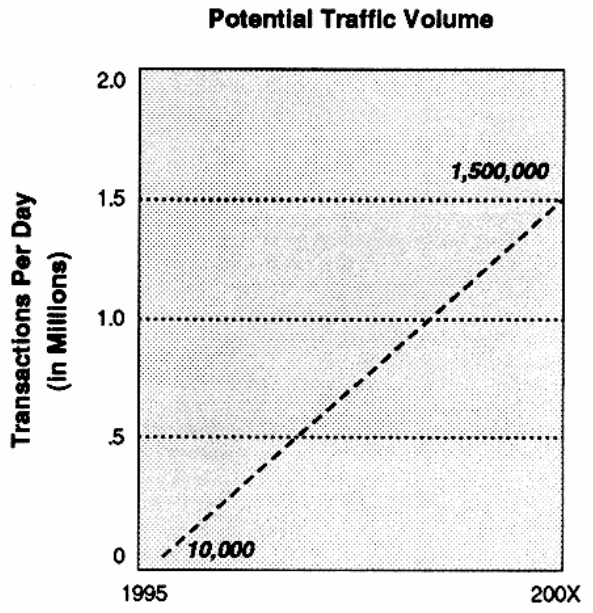



**Figure 29**

**The Future of EC/EDI**

white, we have 50 percent of what we need, and where you see black, we have less than 25 percent of the bandwidth we need. We took all the requirements from all the war-plans, all the requirements from everybody, and that's what we modeled. So, to turn the white and the black to gray, you need the commercial satellites I just told you about. You need Milstar. You need DSCS (Defense Satellite Communications System). You need fiber. The solid black represents the total requirement, so we could

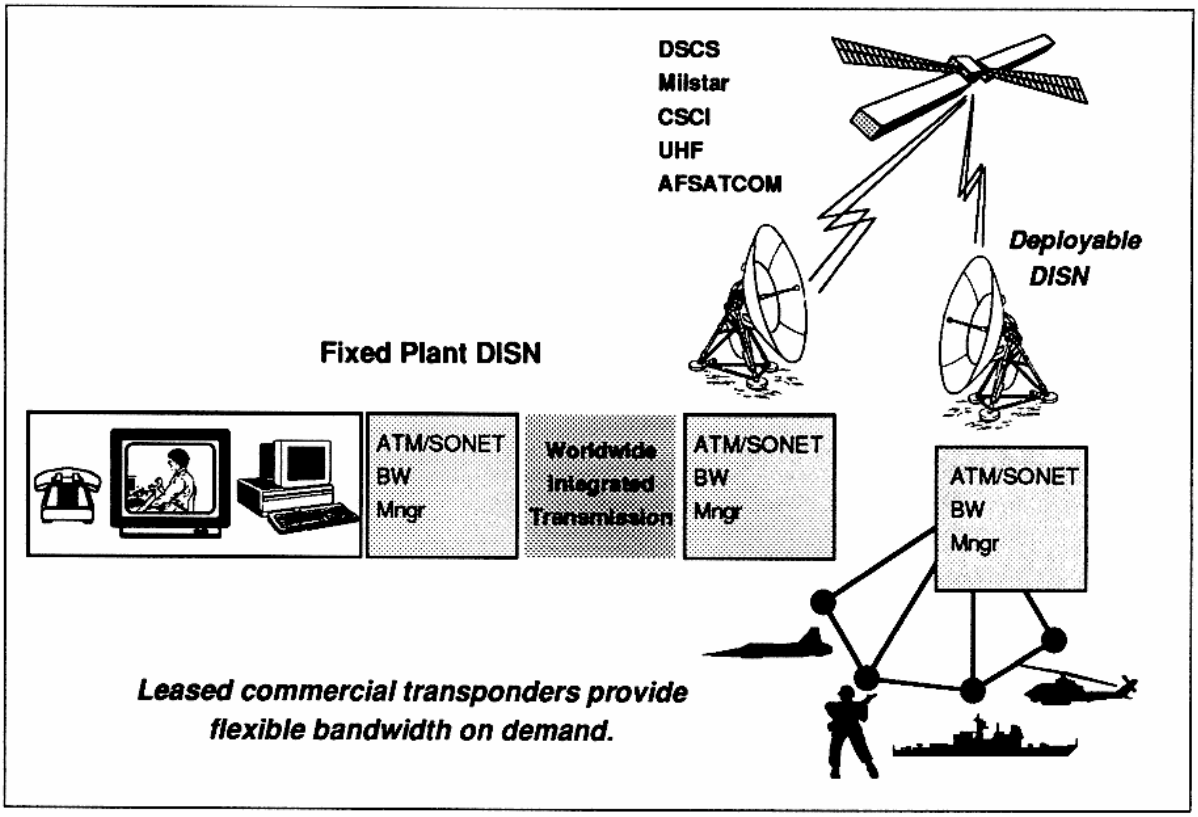



**Figure 30**

**Commercial Satellite Communications Initiative (CSCI)**

show you by day how good or bad you are. This is not just a static tool. This is a real live tool that we can use to model every day and tell you what we need to do to make it better.

These guys, DITCO, the Defense Intelligence Technology Contracting Office, are the ones responsible for contracting for all that stuff we're talking about—the worldwide capability (figure 32). I just want you to know about it. They're on the World Wide Web. They do $847 million in new contracts. They're about a $3 billion or $4 billion dollar business.

I just want to introduce you to the White House Communications Agency (figure 33). They take care of the President and all of his communication requirements every place, and during election time, like this year, we have detachments at Luke Air Force Base, Arizona, a detachment at Camp David, Maryland, and a couple of other places in the nation, and we also take care of other candidates. It has all the capability in the world, anywhere the President goes. We take care of his teleprompters and the Christmas tree lighting on the Mall every year. One year the commander got fired because the lights didn't come on when he pulled the switch, and so now I have guys underneath holding the wires. But we do this also.

**Student:** Sir, let me ask you a question. They work for you? That's part of your organization?

**Edmonds:** Yes.

**Student:** How big is that?

**Edmonds:** About 1,000 people, who cost me between $50 and $70 million a year. People always choose to go there because those jobs are in demand. They're very good. People stay too long. Somebody

**Responsibilities:**

- **Worldwide focus**
- **Long haul communications**
- **Mega Centers**
- **IT equipment/services**

**$847M in contracts in 1995**

- **New contracts**
- **Contract mod**
- **Credit card purchases**

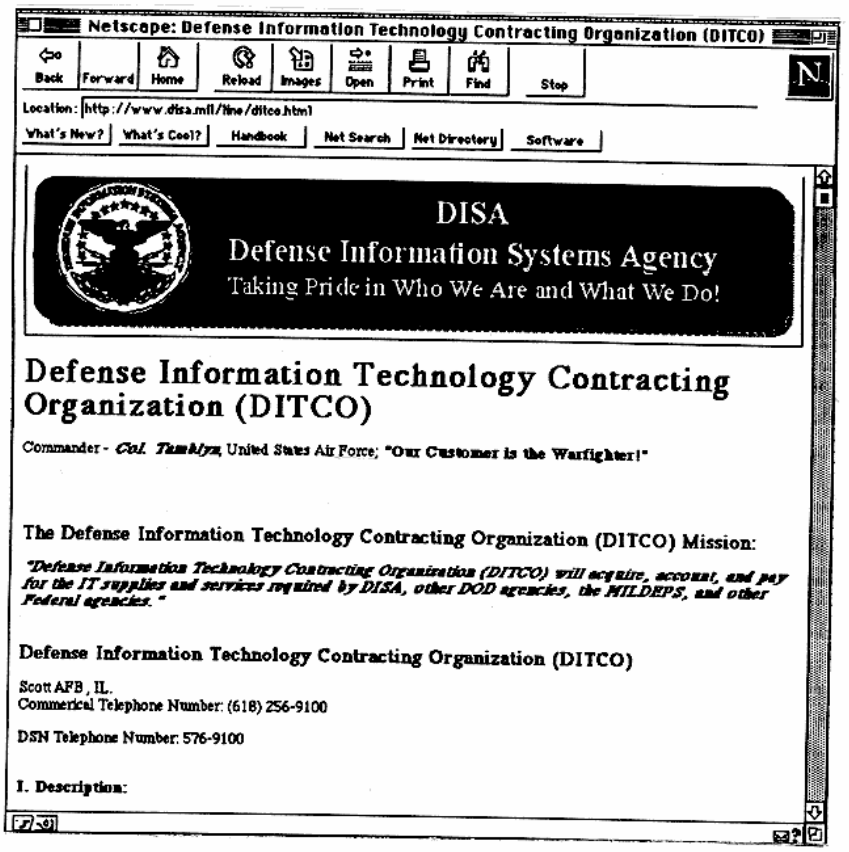



**Figure 32**

**Defense Information Technology Contracting Office—DITCO**

**Worldwide, deployable communications for the President**

- **Both operational and administrative communications:**
  - Secure voice
  - Fax and imagery
  - Computer data

**Complete audio/video support to the President**

- **Recording and archiving all public appearances**

**Figure 33**

**White House Communications Agency**

do what the President tells you to do, and if it's not right, we'll take care of it.

This has been a tough agency to manage since Lyndon Johnson, really. They go everywhere with the President, and they pay their bills. They need communications today, not tomorrow. Yesterday, I didn't know what they were going to do. I hated to see Secretary Brown's crash happen, but we were struggling because they wanted to put a live link between Russia blowing up a bomber and the U.S. simultaneously blowing up a missile silo. They said, "Don't tell the Russians about it until we get this stuff up and are doing it." These guys were trying to make it happen, but they didn't know exactly what was going to happen at the site out somewhere in Russia. That's the kind of requirements they get all the time.

The President of the United States, at a time of national security and emergency preparedness, has authority for all the communication systems in the country to come under his purview (figure 34). That authority has been delegated to the Secretary of Defense, and that has been further delegated to me as the manager of the NCS. What that really means is that, at a time of national disaster and emergency preparedness, we take over and manage AT&T, Sprint, MCI, and all these systems they own and charge you money for, in case we need to. During the Oklahoma bombing, the hurricanes, those kinds of things, we did that (figure 35).

One of the things that came out of Oklahoma was that we didn't have any telephone lines, so everybody was using their cellular phones. So now we have to go before the FCC and try to get them to give us priority on the cell systems so we could establish priority for cell phone calls in times of natural disaster and emergencies, because it would get absolutely clogged up. We have the authority to say, "Okay, *you* get to use it, and *you* don't. You, Interior, can use it; you, Red Cross, can use it; or you, the FBI, can use it. *You* don't get a chance to use it." That's the authority we have. The system covers all of the federal agencies, and since we broke up the Bell system, we have companies that sit in our building to help us when we need to get something, for instance when we needed to put a telephone switch down in the Virgin Islands when there was a hurricane down there. We called MCI, and they had the only switch that you could take in the airplane, a C-130. We sent that telephone switch down there. We called it out; we paid for it.

**Today:**

- **Meet the critical telecommunications requirements of the federal government for NS/EP under all circumstances.**

**Tomorrow:**

- **Promote network security, interoperability, reliability**
- **Help develop and defend the NII**
- ***Information assurance***

***Industry partnership is critical***

**Figure 34**

**National Communications System**

**Responded to several disasters:**

- **Oklahoma city bombing**
- **Hurricanes Marilyn and Opal**
- **Kobe, Japan, earthquake (consulting)**
- **Northridge, California, earthquake**
- **Northwest flooding**

**Activated the National Coordinating Center (NCC) three times over the past year**

- **Responded to several disasters by coordinating additional cell site capacity, satellite and phone bank support to Virgin Islands.**
- **Coordinated first U.S.-Canada mutual aid agreement in support of northwest flood recovery efforts**

**Figure 35**

**NCS Disaster Responses, 1995**

The National Coordinating Center is where I call the companies in: AT&T, Sprint, Motorola—anybody who has something that they can contribute, and they work 24 hours a day. We don't pay them; the companies pay them to coordinate support to any place in the United States or in the islands. Also, up in the Northwest, where we had flooding about a month or two ago, we coordinated support from the Canadians coming across the border to help us. We couldn't get people there, and they did all the splicing for us.

**Oettinger:** What I find fascinating, if I might just add a little historical comment here, is the nonchalant way in which you sort of take this as a routine thing. One of the major arguments prior to the divestiture of AT&T in 1984 was that for a unitary organization that is a monopoly and so on, this was all impossible. You'll note that in this presentation there's no comment; you're just doing it.

**Edmonds:** Absolutely. They all come to know that, and so when we want something, we call and we get it.

So you have a feeling for this, we've also created an about $30 million a year system called GETS (Government Emergency Telephone System) (figure 36). Now you might say, "What in the world is that?" We've gone into all these public switched networks, and all throughout these systems, and issued GETS cards. At the Oklahoma bombing, we issued these cards to the folks, and they made phone calls, and we, DOD, we, DISA, paid the bill.

GETS also includes what we call enhanced routing and priority treatment for national security/emergency preparedness, wherever it's based, and we've got an access code for it. What it basically means is that I get through that system when nobody else can get through; all these switches, all over the country. I don't care whose they are, whether it's Sprint, MCI, or AT&T. If there is one line left, I get it. I authorize who in the government can use it, whether it's Interior, State, Defense, or the White House. We've done that between the big switches right now, and that's this access code. I had to make the first call on this to the White House.

We're now working the local access part of that. We have a contractor called GTE who works with all three of those carriers to make sure this is happening right. Now GTE is also working with these local mom-and-pop telephone companies to make sure we get local access, so we can get all the way down to each location, because that's the other part of it.

We are responsible for that. This exists today. Here is my card, as the manager of the NCS. I've got my number, I dial it in, and only I can use this. Before anybody else can use this card, under these conditions, we, the NCS, have to authorize it. It doesn't make a difference; you can be the FBI, and we still have to authorize it. But you get through and nobody else will. If there is one line, you get it. That's very critical. So that's part of our other

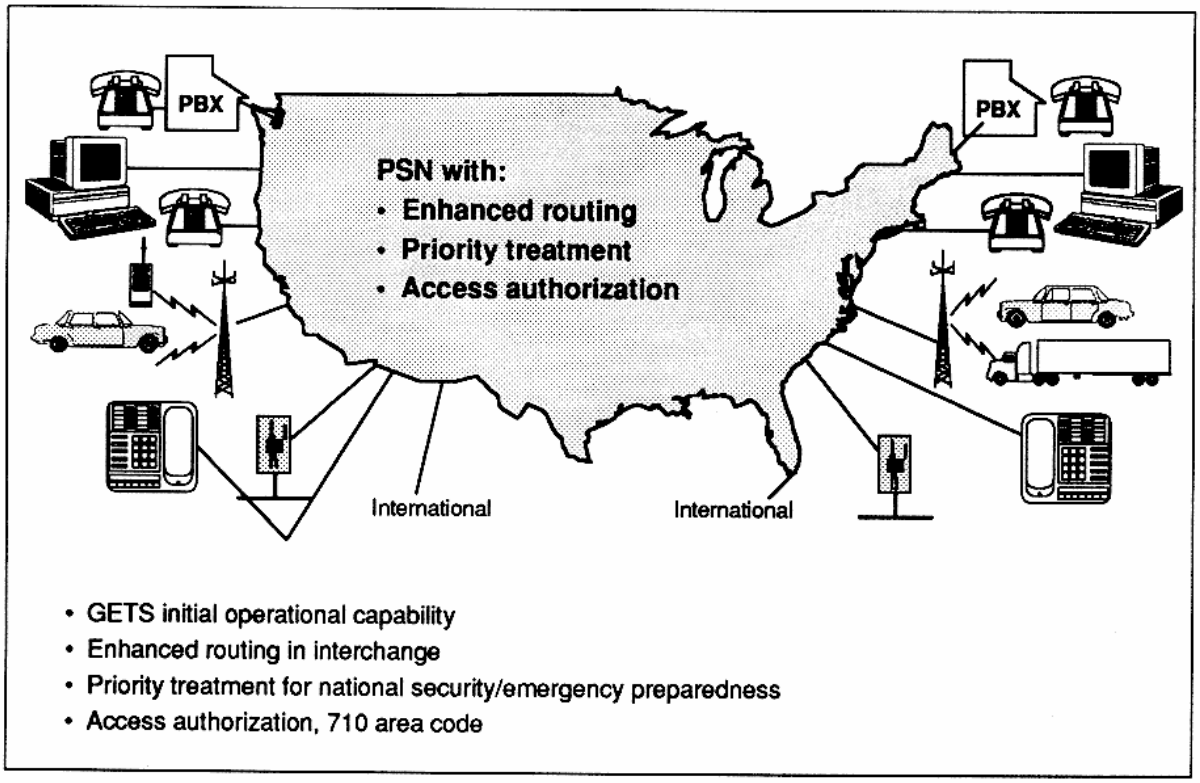



**Figure 36**

**Government Emergency Telephone System (GETS)**

responsibilities. It doesn't make a difference whether it's a natural disaster or emergency preparedness, we just do the job.

**Student:** Sir, are those out around various commands, or does FEMA have them? What's the mechanism for obtaining them?

**Edmonds:** We issue them to those agencies. All those agencies, like FEMA, Interior, and Commerce, have a representative to this thing we call Committee of Principals. We meet quarterly. We deal with all these kinds of issues every quarter. I chair it. The Secretary of Defense is theoretically the boss of their bosses. So what we do is issue these cards and numbers and groups to these Committee of Principals people. For instance, in a disaster like Oklahoma, the President sends FEMA out, he sends the FBI out, he sends a bunch of folks out there. But when that happens, I create my National Coordinating Center, and we are now on the air talking and coordinating all this stuff, and we know who is out there doing what. We get a health and welfare update from these telephone companies to tell us if their systems are damaged or overloaded or whatever. We find out about all the routes and everything else. Then we activate so many of these numbers. We say, "Three of your guys can have this number, you two can have this number, and you can have this one. We know how much capacity we've got to allocate. Only those guys are authorized to use them, and no other numbers are activated." So the telephone company puts those numbers in and activates them. They're ready to go. Then these agencies use them and send me the bill. When we deactivate them, there are no more bills. I use my card sometimes just to check the system.

**Student:** Excuse me, General. Are you also doing the continuity of government communications?

**Edmonds:** We were. A lot of that has gone by the wayside. Some of it is still around, but we've changed the way we do that because of the Cold War connotations to it. We call it something else right now. We're involved in that also. That was a big program for a while.

**Student:** So that piece has changed?

**Edmonds:** Yes, it has changed, and I helped to change it when I was J-6. I was sitting on a TDY (temporary duty assignment) one day—and for five days I could not call my wife—and I said, "I don't want to do this crap anymore. So I have to get rid of this thing." But it really was too awkward, too cumbersome, and it wasn't as good as what we're doing right now.

You know all these things (figure 37). This is the world in the 21st century: virtual command centers, data mining, real-time weather (I'll show you in a few minutes how we're doing real-time weather), and increased jointness. These are just the things that are going to be happening in the next century.

**Oettinger:** Excuse me, is "fire ant warfare" a metaphor or meant to be literal? I was just wondering whether along with drug ...

**Student:** It must be a test.

**Edmonds:** Like cyber snipers? Cyber moles?

**Oettinger:** What on earth is that?

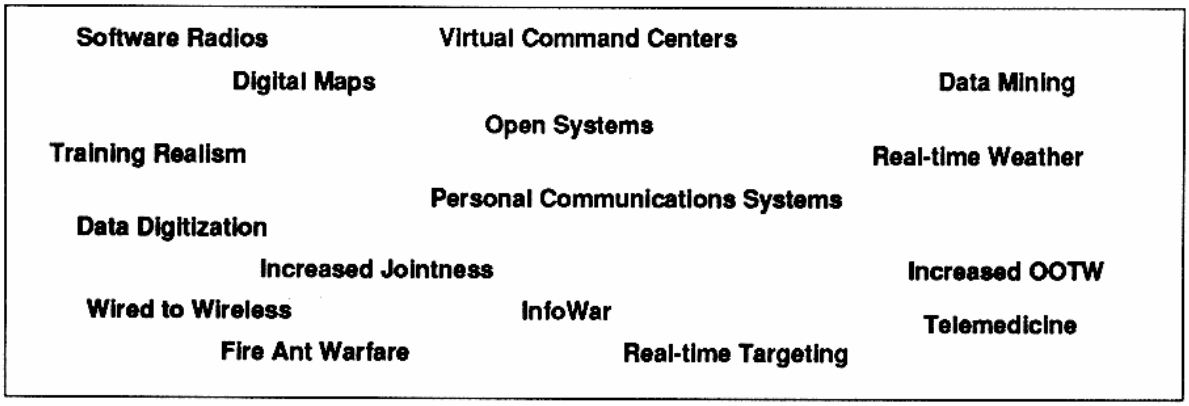
**Edmonds:** It's using cheap, small rockets with one or a few functions. They are very expendable. They can take any shape: plant, animal, insect. And because they are so cheap and numerous, they are expendable.

What I want to kind of lay in here is that digital libraries are becoming a reality (figure 38). We're going to be going to virtual information, virtual command centers, virtual everything. We are already developing the digital dog tag with a complete medical history on it. Even the new ID cards have more information than you ever thought was possible. But secure digital versions of maps and all kinds of stuff are possible today. I hope not too many Army guys are here because the Army guys still like those paper maps. The Defense Map-

ping Agency would like to go to digital electronic mapping, but the Army likes those elevations. When I told the Army to give us some automated maps, they just took the maps and scanned them in. But this is happening.

**Student:** They just don't understand.

**Edmonds:** But the good thing about this is that we are patiently transforming all our mindsets this way. This stuff is happening to us. I went down to my old Air Force last week, and in this operations center, they insisted on having these damn grease-boards. They had these high-priced pilots with their leather jackets on using straight-edges to mark targets and offsets and rendezvous points for the orbits for the tankers and stuff (figure 39). They were having an exercise, and they were waiting for a missile event to come from Air Force Space Command do that TWA (tactical warning assessment) kind of stuff. I asked, "Don't you have GCCS in here?" They said, "Yes." I said, "Then turn it on!" I had already started the missile event over in the joint ops center. And so, there is still a




OOTW = Operations other than war

**Figure 37**

**21st Century Warfighting**

**Digital Libraries**
- **IBM developing optical microscope capable of viewing single atoms**
- **Utility? Incredibly dense storage devices, 100 times greater than today**
- **E.g., *entire Library of Congress on a penny-sized disk***

**21st Century Warfighter Requirements**
- **Digital dog tags with complete medical history**
- **Secure, digital versions of plans, maps, orders, etc.**
- **Graphical, multimedia weapons system documentation**

**Figure 38**

**Data Digitization**

**Old Way**
- **Grease pencil on plastic overlay**
- **Tape maps together for coverage**
- **Inaccurate, obsolete maps**
- **15-year backlog for new maps**

**21st Century Warfighter Requirements**
- **Instantaneous availability, worldwide**
- **Any size, any region, any level of detail**
- **Download maps directly to weapons systems**

**Figure 39**

**Digital Maps**

cultural thing, I'm trying to tell you, of going for what's comfortable. Weapons controllers who used to work in the back of those airplanes just absolutely loved grease-boards, pencils and stuff, and putting those symbols up. They know the symbology they learned, and it's hard to change them.

I used to think that the more junior they were, the easier it would be to change them. It's getting to be just the opposite now. The generals are so overwhelmed with this stuff, they say, "Yes, let me see it, let me see it!" These majors and junior guys want to keep on drawing. So we still have a cultural thing in all the services; we really do. It is just not easy to break the paradigms. And all you need is one boss—one colonel who is a brigade commander, or wing commander, or whatever—to say, "I'm against something," and everybody on the base absolutely refuses to think beyond the obvious. I'd go to one base, and they'd be absolutely way out here. I'd go to another base and they'd say, "Uh, uh, we don't even have any 286s." I say, "Okay, I understand."

I spoke down at Army Staff College about a month ago, and this one major raised his hand and said, "Sir, it's impressive that you've given away $77 million worth of computers to educational institutions in 1995," (which we did; we gave away maybe up to 386s, or maybe a few 486s) "but out at my post I'd really like to get a 286." I said, "Well, you might not be able to get one if you ask me like this, but you might want to give me a note on the side, and let me mail you a few." We sent a pallet of computers to an Army organization in Europe, because the Army person who worked for me is an adjutant in the Signal Corps, and she couldn't get any computers because her boss wouldn't invest the money in them. But the Senators and Congressmen all write to me. I've got equipment on the native reservations, in all the high schools and elementary schools. In Washington, D.C., we gave away computers, desks, everything. We get them for all the DOD, and then we redistribute them. Some of our own people in the department don't have basic computers to do basic stuff. They like doing hard things.

You've heard about software radios (figure 40). We'll go through these pretty fast. I want to get to Bosnia right quick.

The Army has some good training stuff on terrain (figure 41). I saw at the Army organization that's equivalent to the Air Force Association that they had the guys marching and walking, and there's a scope on the soldier's rifle, and he's transmitting that back to the ops center and telling the commander what the situation is. There's a lot of good stuff in this training realism and modeling and simulation.

Joint endeavor support is my next theme (figure 42). Do you remember when I talked about commercial satellites, and using commercial technology to kind of leap ahead rather than R&D? Well, let me just tell you. This is a T-3 big wideband fiber between Washington, D.C., and Molesworth Intel Center that we put in as a

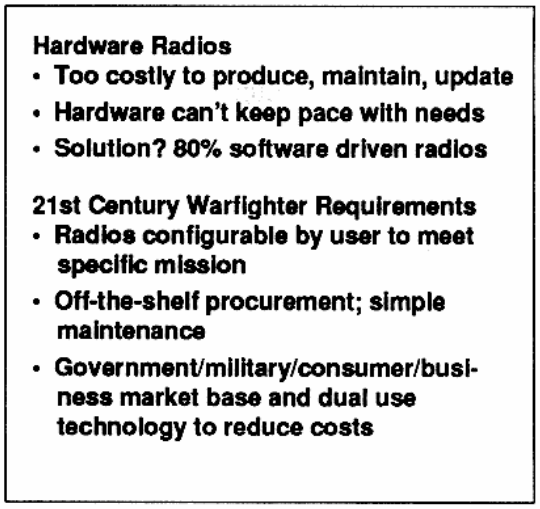



**Figure 40**
**Software Radios**

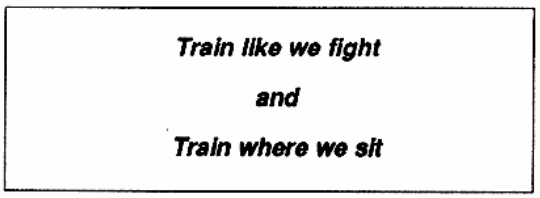



**Figure 41**
**Training Realism**

secondary path. That's to move images. For Molesworth, we are using both the satellite and another system we have, which I'll show you in a minute, to broadcast information out there.

Now, this is going to be on the test (figure 43). This is very, very important. We took folks from Air Force Operations and Air Force Space Command, MITRE people were working with us, ARPA people were working with us, Army people, intelligence, automators, communicators, you name them—about 20 or 24 people—and put them in the injection point in Washington, D.C. We used fiber. I bought a transponder on the Orion satellite from DISA without anybody asking me to, and we were broadcasting from the Predator, an unmanned vehicle, down to the ground site to the Joint Task Force commander, or we could go back through this INTELSAT satellite. We have an INTELSAT ship sitting right here, so we could also go two ways if we wanted to, and when you get down to the broadcast/receive site in Bosnia, you can take it and send it back through to another site. We were doing both broadcast, which is smart push, warrior pull, or two-way communication, and we didn't ask anybody's permission except that of the Secretary of Defense. We briefed them on the concept. They were talking about GBS (Global Broadcast System) and all that kind of stuff, and rather than just kind of talk about it, we just did it.

Next week, the 11th or 12th, we're going to do a real live mission. The Predator is flying now. We recorded this mission, so we can broadcast back here. Look what happened at the inject point! Right down at the Joint Staff we are able to broadcast intelligence, imagery, real-time weather, telemedicine, and we have functional people down there—functional people, not techies—to decide what we're going to put out there, what the warrior needs. The warriors here will tell us what they want. We're going to be broadcasting,

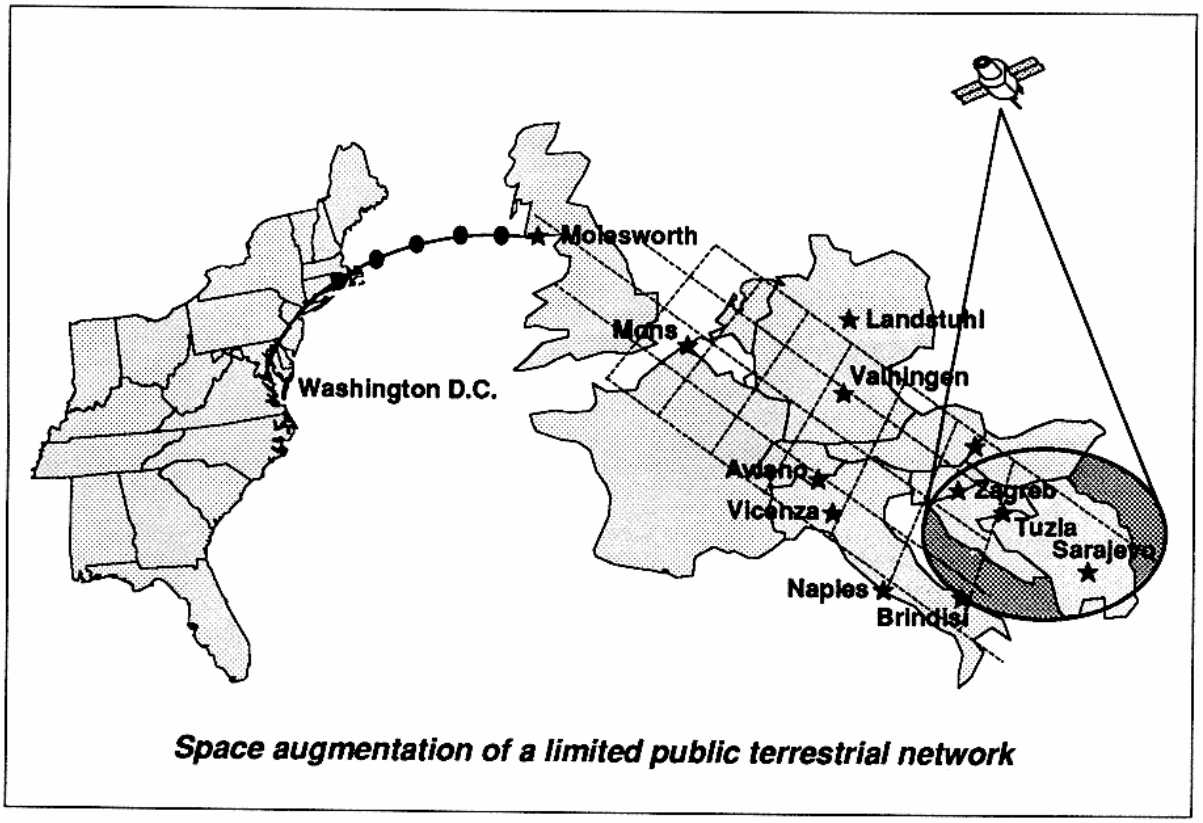



**Figure 42**

**Communications Support for Joint Endeavor**

which is very, very important. We've got the money reprogrammed in Congress. They gave us $77 million to do this. What we're trying to do now is get all the lessons learned here so we can duplicate or replicate this for other CINCs. The only rule we had is that we're going to test it in the States before we put it in the theater, and we've done that. It's really a good-news story: using commercial technology off the shelf, mainline technology stuff, not modifying it, ensuring user involvement, and we're doing it. It was almost too progressive for a lot of people.

**Oettinger:** Just to clarify, Predator is the name of that unmanned airborne vehicle?

**Edmonds:** Yes. We use it both as a platform for communication relay, and for intelligence. I bought a transponder on Orion for broadcast. I bought another transponder on the INTELSAT 602 to use for two-way communications. Once we bought the transponders, I got the requirements. Usually in the past, in this kind of business, we always told the customer, "Let me have your requirements, and I'll go out and buy something once I get them. And, oh by the way, it's going to take 120 days." It became very clear to me that the President said the force is going to be there for one year, so you don't have time to jive around 120 days' lead time. So as soon as he told us we were going to go in December, we went out and bought the satellite. Everybody else said, "We need to buy a satellite." We said, "Sorry, it's already used up. DISA has it." One cost me $2 million, and one cost me $1.5 million—chump change compared with the value we're getting out of it, chump change! But you've got to be able to leap forward and be able to do something rather than plan to do something.

This is the same satellite we're using (figure 44). This is the CSCI bird, the commercial satellite initiative. By my having this contract already in place, when I needed to buy time I'd give you $30,000 and say, "Just reserve my space in that thing." "Got it." I came back and said, "Okay, guys, I got the satellite reserved. Give me your requirements here for what you want to do." The medicine guy said, "I want telemedicine." I said, "You got it!" He said, "I don't have the money right now." I said, "Come back and see me after you get your money. Pay me after the fact." Now they're looking at my agency as something that can provide for all their communications needs. The DISN backbone has been extended out in the area with a lot of bandwidth. I wasn't worried about it. I got $77 million reprogrammed; I got my money back plus more and a lot of good will.

**Oettinger:** I think it's important that you guys read the presentation by his predecessor way back, Lee Paschall, about the problems of getting a DSCS satellite up and maintaining it, et cetera.* Again, it sounds easy today, partly because those commercial birds were up there with excess capacity that he could buy into incrementally, and that's a very different game from having to program for launching a vehicle that is exclusively a defense vehicle. So, in order to comprehend what he just said, go back and read Paschall's presentation years and years ago.

**Edmonds:** Exactly. Then I use the military only when I have to, when I can't get a spot on the commercial satellite, and use it for my tactical requirements or my really critical operational requirement. I could turn it on right now. It's very important.

Let me wrap this up, and then I'll let you ask me some questions.

What I really want to tell you is that we have found the best value comes from healthy competition (figure 45). I mean that in a lot of ways. I don't mean just value for dollars, but value in terms of quality. For a long, long time, we in the military were convinced that we had to have this special unique thing with the funny kinds of warts on it to have good value. I would submit to you that you don't just get the 80 percent

* Lee Paschall, "C$^3$I and the National Military Command System," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1980.* Cambridge, MA: Program on Information Resources Policy, Harvard University, December 1980.

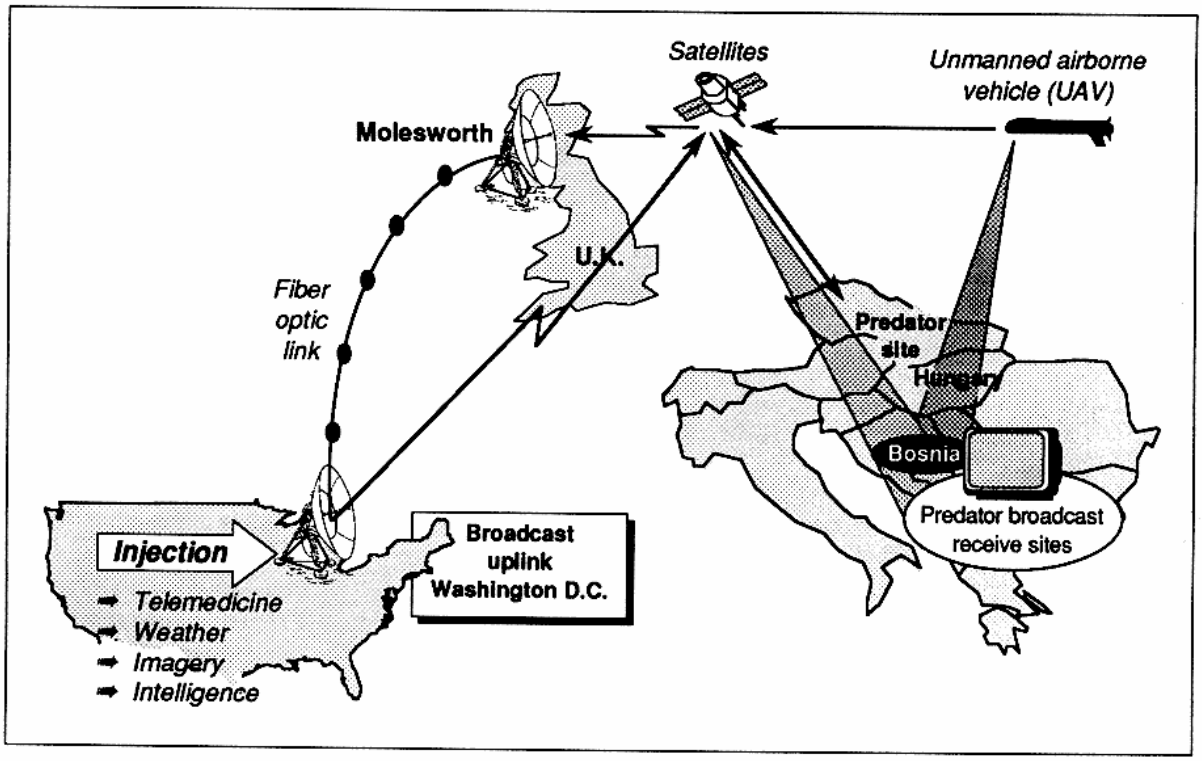



**Figure 43**

**Bosnia C2 Augmentation**

solution sometimes; now you get the 95 percent solution, or 98 percent solution,and it's not worth putting in any more money for the other 2 percent. Don't waste your time on it.

The other thing I would tell you is that you have to have teamwork, in the sense that you cannot worry about who gets the credit. We still have agencies and organizations that don't want to play unless they lead, or have it be their program. The reason why we were able to do this thing out in Bosnia was that no one wanted to give it to the intelligence community to put behind the green door, because you couldn't get access to it. We're trying very hard in everything we do to keep it unclassified. It used to be that you couldn't even say "NRO" (National Reconnaissance Office), but NRO itself was declassified years ago. Teamwork is okay, and I just moved some WWMCCS computers out of the way and bought some terminals and some big-screen displays, and told the folks to go down and get at it. Give it to an ARPA guy and our guys, and let me know when you're ready.

Interoperability is crucial. You really need to make sure that these land, sea, air, and really space networks all come together somewhere, somehow, under somebody to make sure you can take advantage of the maximum capacity available to everyone. Somebody has to be in charge of allocating that bandwidth. When I was J-6 in CENTCOM, I thought that was my job, and never would I have let all that stuff happen in Desert Storm the way it did. If I had been J-6, I would have turned them off. But in order to turn them off, you've got to have some ability to put something in their place, and we didn't have those tools. That's why the commercial satellite thing became very important to us. They give you a set of tools, and you can get people bandwidth in order to buy their own equipment.

I'm also going to make sure I get some stuff that can deploy on commercial airplanes rather than C-141s and C-5s, because you have to get in line to compete

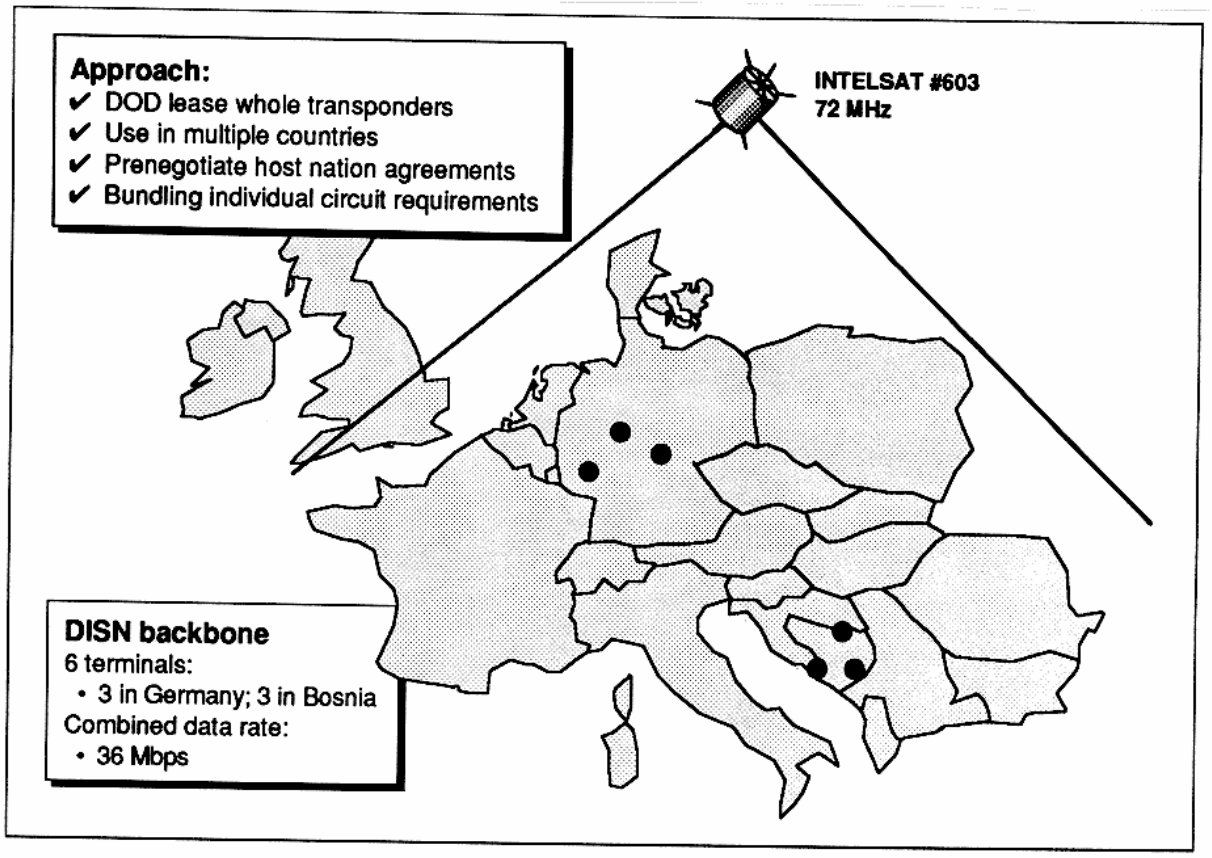



**Figure 44**

**CSCI Support in Bosnia**

- **Best value depends on healthy *competition***
- **Success in 21st century depends on *teamwork***
- ***Interoperability* vital for synchronization of combat power over land, sea, and air (and networks)**
- **Warfighter *requirements* are key!**

***Excellence, when it doesn't change, becomes obsolescence***

**Figure 45**

**Summary**

with bombs and bullets and spare parts. In a recent exercise, I put a whole red switch in the JCSE, Joint Communications Support Element, and they deployed that to the internal loop exercise down at Camp Grant, Florida, two weeks ago, and it worked like a charm. Now I'm going to try to put some in the 11th Signal in the Army, and try to get the Air Force to buy some of their compact comm units, because they are all little suitcases you put in the cargo bay of a commercial airplane. So you have to take advantage of these networks in an interoperable way.

But in order to take care of the warfighters' requirements and not just get a list or a document that has a Statement of Need or Requires Operational Capability on it, we have to have user involvement. Right now we're working to release the ability of GCCS to the Canadians. I'm going to send a team of five people up to Canada to sit down with the customers and say, "How much and what kinds of functions do you want to do with this thing?" So we keep them involved as we evolve their requirements. Once we get that set, we're going to make our deal with them, and we'll open a

foreign military sales agreement for that. Foreign military sales money will help us pay for upgrading and improving GCCS, because we've done the work for the U.S. already.

**Oettinger:** You are permitted to keep that money? You don't have to turn it over to the Treasury Department?

**Edmonds:** No, as a matter of fact, because of what we're doing, and because we're leaning so far forward with our programs, even the OSD comptroller is allowing us to keep money that we've generated from these kinds of initiatives to pay for improvements. For instance, now, as we go out for DISN, I negotiated a contract with AT&T, like a bridge contract. The other contract expired in February. In that contract I got all my terminating liabilities, so I don't have to pay for anything I turn off. I'll be receiving about $2.5 million a month discount, or dividends, or savings, on this contract because I just told them they were charging us too much. We're not getting credits; we're getting checks with our name, the Department of Defense, on it. Every one we get in, we put in an account over at the OSD comptroller's office. We're going to take that money and use it to pay for the Army, Navy, and Air Force costs of transitioning from the current network into the new network because we didn't have any money. We had $100 million we already spent with false starts, so, when I got ready to do these programs, we had no money. They allow me to save money and do this.

On the megacenters it's the same way. Our prices are going down drastically every six months, and as we go down, the Secretary now says, "Let Al keep doing what he's doing because we're trying to save more money and save more people." We got the people down under 2,000. We're going from 9,600 people running the megacenter down to 2,900. Our costs are going from $1 billion a year to $500,000 a year. We're reducing the number of contractors in those things from 690 down to 40, and that's saving $37 million a year. Those are just the kind of things you do every day. You wake up and say, "What can I do today to save more money?"

**Oettinger:** Have I got a deal for you! The People's Liberation Army is running one of the PRC's comm systems as a competitor to the others in order to support itself.* What an ideal joint venture!

**Edmonds:** That's not bad.

**Oettinger:** Easy alliance!

**Edmonds:** That's right, easy alliance. That's the kind of thing you can do if you just sort of lean forward and stay ahead of the competition.

I just want to let you know that almost everything I told you today, with a few exceptions, is on the DISA home page (figure 46). You get everything you want to know about any of those programs on our home page. You find out who is doing all these things for us. You see who can do things for you, with telephone numbers. You name it. We've got data elements on the air. We had two sets of data elements when I came here the first time, about a year and a half ago. We now have 10,600 standard data elements that are free. They're on the World Wide Web. We'll get you a CD with them on it. If you're going to develop any software or migrate any systems, those are available to you. All you do is go in and pull them down, or we'll mail them to you. You don't have to go out and worry about it. We encourage industry to do the same thing. If you have a common operating environment, we'll give you the documentation for the common operating environment. We've got a technical reference manual for information management systems that's available to you on the World Wide Web, and we'll show you how much of that you need to be interoperable with us. Almost everything I've told you, in terms of the tools we have available, like CASE (computer-aided software engineering) tools for software development, is available to you. You can buy them cheaper on our

* Xing Fan, *China Telecommunications: Constituencies and Challenges*. P-96-4 August 1996.

**World Wide Web**

- **Home Page**
  ***www.disa.mil***
- **E-mail**
  ***(name)@ncr.disa.mil***
- **DITCO bulletin board**
  ***(618) 256-9200***
- **DISA Public Affairs Office**
  ***(703) 607-6900***

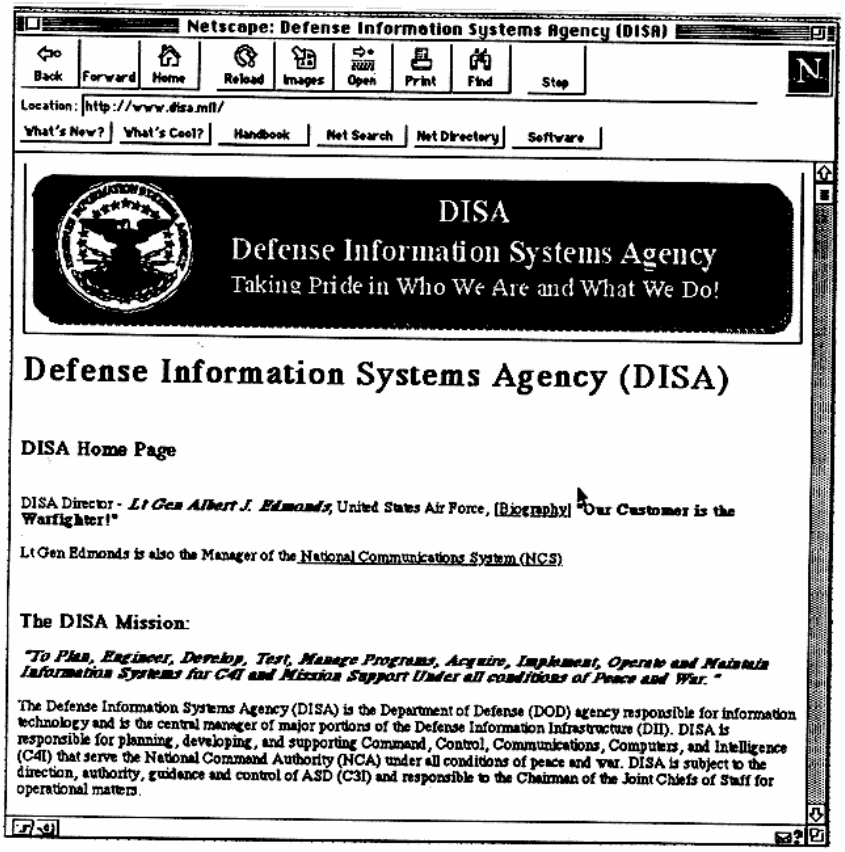



**Figure 46**

**DISA's Home Page**

contract than any other contract you can find. You can expand it beyond the Ada stuff. You get all kinds of tools. It's there for the asking. There's no cost; no strings attached. We've done that because we want to make it easy to do.

**Student:** Sir, I was in Colorado Springs when you spoke out there a couple of weeks ago, and I specifically wanted to ask you a question about the structured threat that you discussed. It occurred to me that we were looking at some executive order that started the National Communications System, and we saw that it said that the Secretary of Defense, as the executive agent of the thing, would seek to build an infrastructure that would be survivable. We know that thing was written with national security preparedness in mind, but are we thinking about information warfare vulnerabilities now as you're trying to fulfill the original tasking that was in that executive order, or building that infrastructure that is survivable?

**Edmonds:** Yes. Under my NCS hat that I have over here, we have a thing called the National Security Telecommunications Advisory Council to the President, and it's made up of CEOs of all the telecommunications companies and companies like Bank of America, IBM, and all those guys. We've done it for the last two years, and we met with the President in February. We have some subgroups in that group. We've already evaluated the telecommunications network in the country and know its

vulnerabilities and the things we need to do with that. We've already done some of that work. Now, because of the Kyl Amendment* that just came out in January, it has tasked the President to come back with a report to say what we're going to do on the other part of the infrastructure, like power, energy, transportation and those kinds of things. We're trying to stay clean in a way, because we don't want to get into trying to tell people to buy power or energy, except how it affects the information technology infrastructure.

But we are engaged with the Bank of America and some of the leading banks on the very same things we are responsible for. I found there's a lot of commonality in it. Those banks and those companies have the same problems I have. I went out to San Francisco and talked to one of the banking people. We went up there at eight or nine o'clock at night, because they were showing me their contingency operations plan. They showed me their off-site processing site. They showed me the security things they use, and we talked about which ones were no good and which ones were good. I found out that a lot of them are still taking the checks and deposit slips at night and doing stuff manually because they want to protect the confidentiality of depositors. They know whom we know.

As a matter of fact, one of the things we're going through right now is trying to find out how we can legally do a vulnerability assessment for some of these institutions around the country, because people are so afraid. They don't want to expose how vulnerable they are, and so they won't ask. They're trying to see if somebody would let us do them. Of course, our lawyers are saying, "You guys can't do this." So we're trying to find out how we can. But the Deputy Secretary of Defense, the Deputy Attorney General, and Sally Katzen, who is the Administrator for Information and Regulatory Affairs over at OMB, met just this week to try to find a way to frame this whole effort in terms of cost to government and cost to the country, both in the President's role as chief executive, head of state, and as commander in chief. Nobody worries too much about the commander in chief part; we can do that with crypto. It's the chief executive and head of state parts that are hard, and they're trying to find a way to be inclusive with this thing without alarming people. So it's kind of happening, but it's been slow in coming because everybody wants to put their heads in the sand and kind of assume it's not there.

But what we do at DISA is that I bring you on site, and if you own the software and I have the tools, I'll show you how vulnerable you are, and let you see it and decide what you want to do. I could help you if I have the tools, but if you don't want to use them, that's okay too. But we'll show you.

**Student:** The 1996 NCS report said that you felt the threat was worse than it was after the 1993 report, and I was just wondering, with the SECDEF looking over the NCS, if he can't be more forthcoming with regards to this, like, "This is the type of technology we need to build the system."

**Edmonds:** We have a problem, and the problem is NSA. I'm kind of the straight guy, the front guy, the white-world guy, for NSA. Nobody in the government, including part of DOD, wants to beat on NSA to give them any products or sell them any products or recommend any products because they think there is a hook in them. So what we're trying to do is convince folks that DISA is okay. NSA is just kind of telling us things, but we're okay. It's this American concern for privacy, the American concern for Big Brother not looking over me. Every time I go in the meeting, even when I explain the kinds of threats to these folks, the last thing they want is DOD being in charge of this thing. And so, about the best I can do is take you over in the corner, one-on-one, and say, "Look, I'm really a good old guy. I've got both a mother and a father, and I won't hurt you, and I'll let you know what I'm doing to you." Then they'll let you help them. I've had a lot of private handshaking with regards to help, and given it on the basis of,

* U.S. Senator Jon Kyl (R) of Arizona.

"Okay, I won't tell anybody, but I'm going to check you, and hand it to you." That's all they're going to let you do, even the services.

I had the Chief of Staff of the Army come over, and I made darned sure of what we were going to look at. I called the brigade commander and the division commander, and told them what the problems were before we showed the Chief, so the Chief wouldn't call and fire the guy. So then we gave the Chief the mouse and said, "Click on this right here, and run the test against this post." He ran it, and 15, 20, 30 or 40 seconds later he saw the vulnerabilities. I said, "Which one do you want to look at?" He clicked on it, and he said, "Oh, my God!" General Reimer said, "Al, my problem is I keep telling all of my generals to use these systems, but if they saw this, they would never use it again." So that's the kind of limit you have.

One thing we pulled off the Army's local area network was a list of people about to be promoted. This, I guess, was last year, 1995, and it is not important except that if the Army had red-lined these guys on Tuesday or Wednesday, I could have called one of these guys and congratulated him for making general. It wasn't classified, but it was sensitive in that most of them were pre-positioned, and almost all of us do that. The Air Force does it. We even put some lists out a week and a half ahead of time, and the administrative guys put it on the LAN, and it shows that it is not important.

There are also some lists that come out of people's e-mail addresses. We look at the country clearance on some of these folks, and based on where they're going, you might figure out what they're doing. But these are things that we pulled down just to show you that we can do it for you. But it's your information, and we'd never do it unless we got permission. One place we pulled down was a civic group in the area, and it didn't seem important except most of them were generals and a few warrant officers and command sergeant majors and others. So if you're a terrorist, and you want to do some terrorism stuff, you could go right to Tony's house. You don't worry about any fallout from hitting three houses and hoping you get him; you will just go to one house, because you know the address. That list had telephone numbers, addresses, a lot of private information in it. It's nobody's fault, it's just where there is a protocol list, they were using it to invite folks to a function on the post, camp, or station.

I have hired 120 interns since I was here last time. They're all out of college, with computer science or engineering degrees. I'm recruiting 300 more right now. I've got 3,500 applicants for those 300 internships, and they're the best minds I could find out of all the schools. I get them on these machines and just let them get at it with these tools. They are just absolutely fantastic. This is just to protect systems; this is not offensive. This is only defense. We sit there and we watch these folks go in and out of the systems and check things. We help you recover. Some of the schools go down, and we help them to recover. We shut them out. We give them tools to lock themselves up. It really is a big thing.

**Student:** I have a question that has to do with some of the same stuff. I'm doing a paper for Professor Oettinger on how adversaries are going to look in and try to make these attacks. One of the things that we were positing might be an obstacle for them is just figuring out things like the standards that you guys are openly publishing on your World Wide Web site. You're making their information problem easier.

**Edmonds:** Well, that's true. We get the crap beat out of us in the government, especially DOD, by having MILSPECs and MIL standards. When you get a new administration, especially when you get a bunch of folks from academia, they are hard over on this sort of stuff. I used to understand when I was talking to a senior person. Every person who comes to the Pentagon wants to make darn sure that when they leave they can still write back in, or call back in, or e-mail back in to the Pentagon. So anything you put in this system to prevent them from doing that, they aren't interested in. They'll be working it as a policy issue, a major functional issue. I'd say, "I know what they want. They want to be able to get in and go out." Nobody gives

their e-mail address when they leave. That's one of the things.

Also, you'll notice, I talk about mainline commercial products. Policy folks are more adamant about this than I am. I wouldn't give anybody anything, but they want to make sure that you go down to Egghead and buy the same thing that they're going to buy, so when they get the right numbers together, they can communicate with you. If somebody had told me four years ago we ever would have given GPS access at the locations that we did, I would have said, "No way!" I fought it when I was a J-6. I fought it forever. When the President signed that the other day, I said, "We're now at the point where things like information about networks and stuff ... shhh! We aren't going to keep it from anybody." So, you've got to get smarter and find other ways.

Now, having said that, the other pressure you get—not all of it from the academics who come to the Pentagon—you get from industry, because industry wants to sell their products. The way you sell American products to overseas locations is to use them yourself. You can sell me an overseas version of the same thing I got for CONUS because you can't convince me that's not good. You might remember the F-20 airplane when Jimmy Carter was President—excellent, low-priced fighter. There were three or four countries that really wanted to buy it, but they had one fundamental question: "Is the U.S. going to fly it?" because that's spare parts, that's training, that's support. If you're not going to use it, they're not going to use it. The C-130 is the most successful airplane we ever built; everybody in the world flies it. As a matter of fact, if you don't have one, you're not a country. Some people use it for their command airplanes, some use it for the head of state, some use it for hauling things, some use it for all of the above. But the fact of the matter is, if you're using it in the U.S., it's okay. If we stop using 130s, they'll go to something else. One of the biggest arguments we hear around Washington, D.C., is on export control on these software security products and stuff. They won't sell them. But until the U.S. people use them, we won't get anybody from overseas to buy them.

So, there's a lot of pressure on us using the same thing everybody else is using, and that's why we had the Fortezza approach and some other kind of way how we can stick this in our machine and protect our secrets and our information so we can use the same other products. That's why Microsoft Exchange and Lotus Notes became so important, because they took the engine for those products, and just put our stuff on top of it, which means they can sell the basic to everybody else, and everybody knows that Defense has to have this thing on top, so it's no big thing. But if we had another version of something, called Microsoft whatever, that was designed for DOD, nobody would buy it. They'd say, "Uh, uh, I don't want that, because they're going to be looking at my stuff." That's the real problem.

Now, having said that, let me tell you one other thing I find. The standards are not as important as database management. The DOD IG went out and looked at my megacenters—I have 16 big ones—and came up with 111 findings. Boy, I started being called every week from the Hill and from OSD asking me to tell them what we have to do to fix these 111 findings. I sat down with my smart folks, like this young fellow here, and he said, "No, it doesn't look right to me. These are nothing kinds of findings. Why are they bugging me about these things?" It's just that they knew that there was a bad situation, but they were using the wrong indicator for the badness of it. I said, "I'll tell you what. I'm going to go look at this thing myself." I hired 30 guys and gals—fresh people—and I sent them out to every one of these megacenters, and told them to go from top to bottom, and tell me what the problems are. We found 4,000 findings, where these guys, who are experts, found 111.

I went back over to brief these folks who were beating up on me, and I said, "Let me tell you something. Don't bother me with these 111 anymore. I've got a real problem here!" and I went down and listed my problems. We put them in categories, because I do things simply. I'm a Columbus, Georgia, kind of guy. I looked at

these categories, and most of them were database management, database management, database management. "I'll fix it today. I'll bring in another application tomorrow. I'll bring in another set of problems." People are trying to go around this system. People bring stuff from home. People bring stuff from the office and put it in there. This is a continuing problem.

So now I will monitor these problems, and I have them all scoped so I can rate my chiefs to see how well they're doing. The first thing I do when I go out there is ask them to show me their security stuff. They bring me their charts. I start watching the graph falling, rising, and falling every time they brought something new to the megacenter. They had a set of problems, and the trend had to go down and come back up again. It will never be fixed permanently. It's a continuing problem.

So I concluded that information security or information assurance is going to be translated to become the current operations for information technology. It is no longer hanging tapes and running machines, pushing buttons. That is not operations. That is something that robots are going to do pretty soon, and certainly is something a few contractors can do. But information assurance and information integrity are going to be the job of the future called "current ops." It won't make any difference whether you're in a command center or a bank, or wherever you're going to be: current ops is going to be information assurance and information integrity, and you're going to build it using some people who are smart enough to understand the data, data structure, and data protection.

If I were a new person coming into this business right now, I would try to understand some kind of operations. I don't care if it's marine ops, or flying ops, or walking ops. I would want to understand some ops, some kind of intelligence, in terms of fusion and analysis, and a lot of information technology in terms of automation, in terms of manipulation of data, and networks—a lot of understanding of networks. That's the perfect person, as far as I'm concerned, for the marketplace of now and the next 15 years. The better you are in all those phases, the better off you're going to be. That's my opinion. I'm trying to take that part of the knowledge that I understand, and give it to this young guy, because he has a lot of a couple of kinds, but he needs about four or five others. I'm trying to make him one of those kinds of guys who, when they make lieutenant colonel or colonel will be able to say, "Yes, I understand this problem."

Today there are hardly any general officers who can talk at this level about this kind of subject. They all will migrate back into their comfort zone and talk about what they know. Either he'll be an operator and just kind of operate you to death and not get involved, or he'll be an intel guy who would just intel you to death and talk about funny stuff that you don't know anything about and don't have a clearance for, or he'll be a software guy who talks about data structure elements, or a comm guy who wants to talk about backpack communications. But you can't get very many folks to talk about this thing in the middle, this new thing I would create. It's information technology. It's information warfare, really. The Air Force calls it the Fifth Dimension—air, land, sea, ground, and now they've added information. That's in the Air Force Secretary's document, *The Fifth Dimension of Warfare*. People don't want to accept this because it's not lethal in terms of blood, but one characteristic of this thing is that you can be a long distance away and do a lot of damage.

Every time there's a hiccup at one of these airports, like the O'Hare radar, I worry that somebody has done something to that radar. Every time an Amtrak train goes off the track someplace, I worry. Every time the lights are blinking at four o'clock on a rush day out of town in Washington, D.C., I worry. I worry about some other things I know are happening. I worry because a lot of folks don't think these things are real, but I can tell you, this is absolutely real.

But we'll get us some tools, and our task is to get our tools ahead of the adversaries. Right now we've got a small lead on them. We need to widen that lead. That's what I would ask industry to do: to give us the tools to detect and protect, primarily to detect, because protection is a false sense of

security, and too many folks think you can close all the doors, and you can't. You absolutely cannot. It's like the Pentagon with thousands of windows; you leave one open and that's enough for us to get in. We do that all the time. That's part of our assessments. Guys come and brag to us and say, "We're good. Check us out." We'll find one system—it may not even be in that building, it might be someplace else—that will get us into that building, and once we get in there, we've got the whole show. It's just as if they left the doors wide open.

**Student:** Sir, but where are the bad guys, if not from industry? Given the reliance on buying off-the-shelf systems and bringing them in from companies and things, I just wonder where technical expertise of an adversary is going to come from but from the people whom we're now relying on for some of our operations.

**Edmonds:** You'd be surprised. As a matter of fact, if you have a brother or sister or uncle—anybody who is 12 years old or above—they're capable or wreaking havoc on a lot of these systems. Almost all the colleges are doing this now. Almost all students are required to bring computers to college when they show up. We've had them in the Air Force Academy now for about 10 or 15 years as a standard issue item in their rooms. As a matter of fact, when I was out at Colorado Springs, one of the cadets raised his hand and said, "I'm concerned about the ethics of us being taught offensive information warfare here at the Academy," as though anybody would care. He said, "But our professor thinks offensive information warfare is where you understand how to do defense." I applauded him for it, but they're not just computer science majors in these courses, it's everybody. That's one thing, but I could tell you that this is not that hard. This is not like when I majored in chemistry. That was hard. This is easy. Ever since my youngest daughter was 10 or 11 years old, I used to give her my watches to set because I couldn't set them; they were too complex. She could beat me in Donkey Kong and all those things way back then, long before we got these complex games. It's a different coordination of mindset.

SATAN (Systems Administrator Tool for Analyzing Networks) is a good example. You've heard about this tool. This tool came out for everybody to use to protect their systems, analyze their own systems. But, in fact, what it really did is gave you the ability to go and hack on everybody's system because it's cheap. Every four-star, three-star, senior executive in DOD I've shown this tool to on our computer system could take this and go hack their own system. They're shocked, because they type about three or four things, and they've gone back and told me how many systems they got into. This is available free.

**Oettinger:** Yes, but where does this fit if I take a scale on which at one end I've got a kid painting graffiti on a subway car and on the other end there's somebody dropping a bomb on New York, Washington, Chicago, and a few other places. Now clearly, these are somewhat different. What I'd like you to do is give me an example of sort of where these people are on a scale from some guy with a spray can to a nuclear holocaust.

**Edmonds:** I'd put another scale in between Oklahoma City and the World Trade Center, because while a few people lost their lives in the Trade Center bombing, a lot of them got it in Oklahoma. In a way, I kind of paint Oklahoma a little bit differently in that it was an internal threat that, in my view, came from a warped mind.

**Oettinger:** You pick the scale.

**Edmonds:** Somewhere in between the World Trade Center bombing and Oklahoma. Let me tell you why. There's no doubt in my mind that they could do as much damage screwing up the air traffic control system around Boston, up at Logan Airport, in peak traffic by taking that system down as they did in Oklahoma City, because if you attack several of those air traffic control systems that you use as alternate bases, so that you couldn't land airplanes without other chaos, you'd have problems.

**Oettinger:** If you screw up the alternate airports, then you've got a real mess.

**Edmonds:** Exactly. The real issue here, and this is the real debate and discussion, is how you decide when you really have a threat of a crime versus a threat of warfare. Let me show you something (figure 26). Remember the time I stole the chart from this guy in Washington, D.C.? That was a guy at the NSTAC (National Security Telecommunications Advisory Committee) who had a chart that looked like this, and he was talking about switches, public switched network kind of stuff. He said, "This represents one switch, and this represents all public switched networks. When do I decide that this is a problem: when somebody tries to screw up one switch in downtown New York, or when I find out that all of the public switches are under attack by somebody and we know we have a strategic attack on our public switched network? Somehow, some way, we have to define intellectually how to decide when this is just a criminal doing something because he's pissed off because he lost his job by downsizing or whatever, or when somebody's trying to disrupt our whole way of life. Where on the scale do you draw that line?" We have not put our intellectual powers and energies behind this because nobody wants to admit that this is a real problem.

It's the same thing for a bank. When somebody from another country is moving a lot of currency, how many millions of dollars is it going to require for you to decide if it's a crime versus an attack? Is it $50 million a day, or is it $100 million a day before you decide this is an attack on your banking system? Or is it a crime, like when somebody is trying to get some money from you? I think if you tried to move $2,000 out of somebody's account using a PIN number or whatever, you'd probably fall into the crime category, but if I'm sitting over in Livonia trying to move millions of dollars from here to Switzerland to a numbered account, you might wonder if this guy is trying to get rich or if this guy is trying to get some money for the state. That's the problem: this scale here and how we're going to define it. The people who are responsible for defining threats, or threat analysis, and giving you a threat estimate, won't engage in this until you have a smoking gun. Until they get somebody and get evidence and proof that Cuba or somebody they have on a list of countries they consider "not friendly" is doing it, they won't deal with this at all.

We were watching a case not too long ago, and we got some data on the characteristics of the person doing the work. It gave us this feeling that this may be one of those nation state kind of threats we've been looking for, except it happened during normal duty hours and class hours, and came from a school. So maybe it's a student just trying to do a research paper for his class, but he's doing a hell of a job. I'd give him an A right now. But we're going to make sure that's what he has in mind, because if not, we're going to try to arrest him. That's the kind of intellectual discussion people won't engage in.

**Oettinger:** Break-ins, break-ins ...

**Edmonds:** A lot of folks talk about it, but they won't say, "Let's call this something and put it in a category until we prove otherwise." You need tools to prove that this is not a crime, but it is warfare. I know what we're capable of doing, and I won't talk about what we are capable of doing, but I know we're capable of doing it. This could be warfare as well, depending on what we're trying to do. I can take any industry and tell you the same kind of thing. So, that's the real problem.

**Student:** Just quickly, on that issue of drawing those boundaries, I've discussed it with people, and it's both a matter of numbers of switches or numbers of dollars and a matter of intent. Is it a foreign actor? Is it financial in intent? Is it criminal in intent, or are they trying to influence our policy?

**Edmonds:** Yes, and that's the difficult part. Where do you put a disgruntled worker who just got laid off as part of downsizing and goes into his software before he leaves and puts a Trojan Horse or something in there to take your whole infrastructure down, so that you are unable to

function as a company or to pay your bills while you recover? Is that a criminal act or is that some kind of information warfare? And, oh by the way, what is his motivation? If he's an American citizen, you probably want to call it a crime. But I don't know what you'd call the Oklahoma City bombing. Isn't that an attack against the state, when you bomb women and children because you have some fundamental problem with your government and some other stuff I hear people talking about on television, about the government is not legitimate? Some folks got killed for that kind of thing not so long ago in this country because it was thought they were plotting to overthrow the government. There were 15 or 20 people, and they were saying those things publicly. But now we negotiate those things, and discuss them. You want to talk them out, because we had a couple of incidents out in Waco and other places.

When is something a crime? You see, I've sworn to defend the Constitution against all enemies foreign and domestic. So when does a domestic action become an enemy action? There's a lot of philosophical discussion in here that you just can't pull away from. If I do something to take down the air traffic control system, or the power grid, or the infrastructure of this country, even though I have an American citizenship card in my pocket, when is that not just a crime? When is it treason against the state? No one is bothering with that kind of dialogue because it's frightening—there are 12- and 14-year-old kids with zits who can do that. It might be your son or my daughter, and they might do it for kicks. So that's kind of foreign to us.

**Oettinger:** One of the first who got jammed for that was a Harvard graduate.

**Edmonds:** Exactly. There are folks who have philosophical differences with what our government does from day to day and would do anything to make that point. I don't know how you should treat those folks: as criminals or as traitors.

**Oettinger:** I hate to put a stop to this, but we promised ...

INCSEMINARS1996

ISBN-1-879716-39-9