

INCIDENTAL PAPER

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

**Providing Global Information Services to the
Warfighter**
David J. Kelly

Guest Presentations, Spring 1999

Charles J. Cunningham, Kawika Daguio, Patrick M. Hughes,
Peter H. Daly, Walter Jajko, David J. Kelly, Gregory J. Rattray,
Michelle K. Van Cleave, Robert T. Marsh, Randall M. Fort

June 2000

Program on Information Resources Policy



Center for Information Policy Research



Harvard University

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

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

Copyright © 2000 by the President and Fellows of Harvard College. Not to be
reproduced in any form without written consent from the Program on
Information Resources Policy, Harvard University, Maxwell Dworkin 125,
33 Oxford Street, Cambridge MA 02138. (617) 495-4114

E-mail: pirp@deas.harvard.edu URL: <http://www.pirp.harvard.edu>
ISBN 1-879716-63-1 **I-00-2**

Providing Global Information Services to the Warfighter

David J. Kelley

On July 27, 1997, Lieutenant General David J. Kelley, USA, became the director of the Defense Information Systems Agency (DISA) and manager of the National Communications System. In this position, he is responsible for providing command, control, communications, computers, and intelligence (C4I) support to the nation's warfighters. Previously, he had served as DISA vice director and then as acting director until he assumed his current position. General Kelley was commissioned in 1966; his military service has included several tours of duty in Europe and in Vietnam, as well as increasingly responsible command positions in the United States. His most recent European assignment was as deputy controller, central operating authority, Supreme Headquarters Allied Powers Europe. He became deputy commanding general, U.S. Army Signal Center and Fort Gordon, in October 1990; a year later, he was assigned as director of systems management, Office of the Director of Information Systems for C4, Secretary of the Army, and in April 1993, he became the vice director for C4 Systems (J-6), the Joint Staff. General Kelley earned a B.S. degree from the U.S. Military Academy, and M.S. degrees in industrial engineering and in computer information and control engineering from the University of Michigan; he also completed the College of Naval Command and Staff, and the U.S. Army War College. His military awards and decorations include the Defense Distinguished Service Medal; the Defense Superior Service Medal, Legion of Merit, Bronze Star Medal with oak leaf cluster, Meritorious Service Medal with three oak leaf clusters, Army Commendation Medal, Parachutist Badge, and Ranger Tab.

Oettinger: Our speaker today is General David Kelley, who runs the Defense Information Systems Agency (DISA). It used to be the Defense Communications Agency. Anyway, we're delighted to have him with us. You have his biography, so I won't go into any more detail about him. Today he's accompanied by Mr. Peter Paulson, who is the chief of DISA networks. Sir, it's all yours.

Kelley: Thank you. Because we come from an organization that's an acronym soup—DISA—I thought I'd just talk for a few minutes on its background so that you will know what we do and what we are (figure 1). Then I'll get into the programs and some of the issues that we're dealing with today in command and control and information assurance and protection. I'll also get into the pillar programs to let you know how we're implementing the mission we've got.

I brought Pete with me because we're going to take one example that sort of leads over from the military aspect into the civilian

infrastructure. He's in charge of all our networks, but a large amount of what we do for the folks in Bosnia and the Pacific and across the globe is, in fact, dependent on commercial networks. AT&T, MCI, and Sprint are three of my biggest contractors. So I thought I'd use them as an example and just give you a few snapshots, and then I'll have Pete give

- Background
- Battlefield pull
- Pillar programs
- Information assurance
- Interoperability
- Menu items

Figure 1
Agenda

you the select overview for about 20 minutes or so. Feel free to interrupt and ask questions. We'll give you a menu at the end to get you into anything that you want to talk about. I've put some topics up on the menu, but we'd certainly be willing to entertain any questions that you might be interested in. So with that, let's go ahead and move out very quickly.

The agency I run is a combat support agency (figure 2). A little-known fact is that I have about 800 soldiers, sailors, airmen and marines who work for the President of the United States. Any time he travels, some of my people travel with him. They're responsible for providing communications to the President under his authority as the head of the military, so they're with him at all times. They work in the White House. They answer the switchboards in the White House. They took photos of the coffees that were the subject of intense discussion in Congress some time back. They knew nothing, and they were innocent ... and that is our answer on

any of these political topics that come up. They're not political. In fact, they're there just to serve, and they do take guidance from the White House staff as to whom they should photograph, or what they would do in the tasking for the President.

Below that, at my organization in Arlington, Virginia, I have a staff set up very much like the Joint Staff, where the D-1 is similar to the J-1 on the Joint Staff who does personnel, the D-4 does logistics, and so forth. There are a few differences, but I did that because nobody could really understand what the agency did, so we used some sort of analogy to make it easier for the military folks. I have several different bosses, but the Joint Staff is a large portion of my boss group.

Below that, I have field offices and commands that work for me scattered across the globe. I'll show you that on a map later just so you can pinpoint where the agency is, because it's not just a Washington agency.

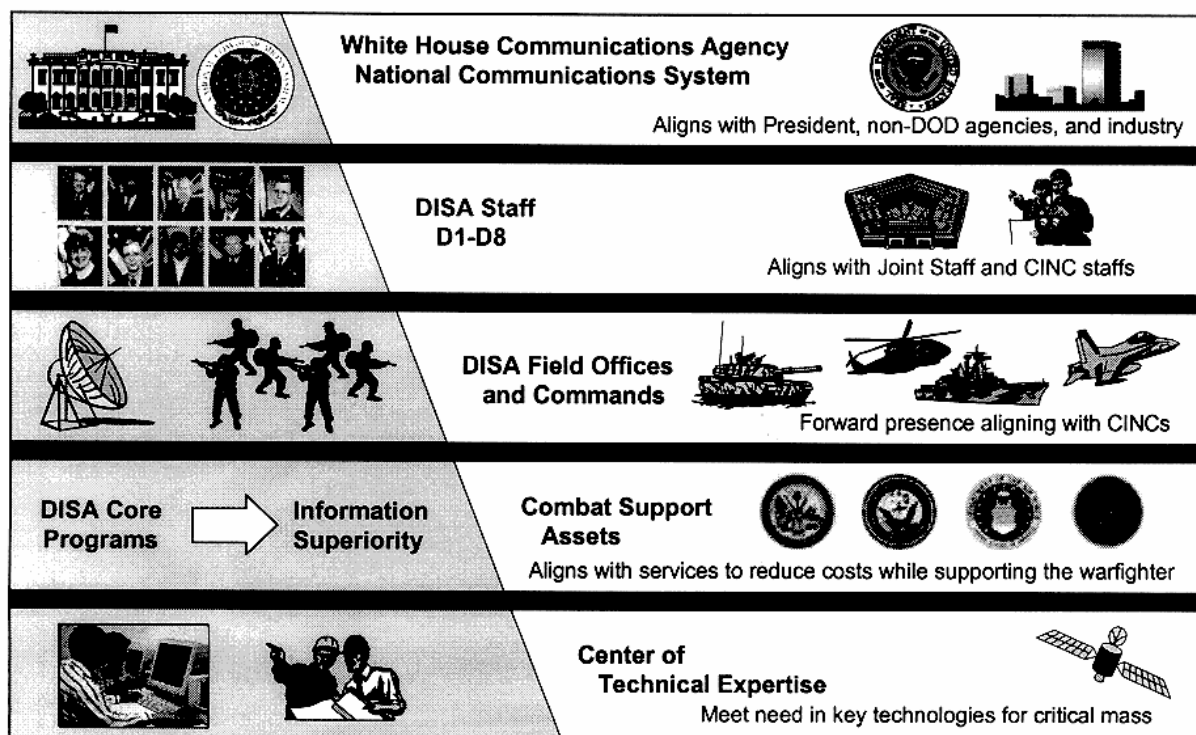


Figure 2
**Defense Information Systems Agency
Combat Support Agency**

Below that, we have these core programs. Pete runs one of the largest. We just finished switching out the infrastructure for the transport layer in the United States. Now it's all fiber optics, the synchronous optical network (SONET). Pete ran that action for me. In fact, he's expanding it out to the Pacific and into Europe, so he'll be going through that in some detail.

We also have several other programs that we'll talk to you a little about, and depending on your interests, we can go into them. The Global Command and Control System (GCCS) is a system that all of our commanders and chiefs use to synchronize combat power. It's being used right now in the situation overseas in Kosovo. The corollary to that system is the Global Combat Support System (GCSS), where we try to bring the whole logistics picture together and to make it interoperable. This has been one of our biggest challenges, and one of our main purposes for being is to get at interoperability. We'll get into some of the problems involved in achieving that goal that we face today in spite of all the lessons we've learned through our various deployments.

On the bottom of the slide are the centers of technical expertise. I have a very large engineering organization. My chief technology officer is Ms. Dawn Hartley. The engineers' task is to take a look at technology and the directions in which it's heading, and make sure that we're working in our labs with that technology so that we can inject it into the networks that Pete runs in a timely manner, and we always stay one step ahead. The labs are a very important piece of this. A large number of engineers work in them. They're mainly located in the Washington, D.C., area, Virginia, and a few in Maryland.

This is a people chart (figure 3). Back in 1992 we started with about 14,000 people, and that was when the message came out that we were going to downsize the military. That actually started after the Berlin Wall came down in 1989. But we've got a spike in 1993 because we got a whole new host of missions. This is when we took on all of the processing in all of the megacenters. We do large, mainframe computer processing for the Department of Defense: finance, personnel, logistics, and maintenance. Those kinds of applications came to us. That's why we

spiked up from this 5,000 level. From that spike, we've been working it back down, based on efficiencies and reductions in personnel, to where we're at about 8,500 to 8,900. The number of personnel we have fluctuates in that range. That's military and civilian. You can see we're largely a civilian organization. We have military staff, not in large numbers, but in sufficient numbers to bring the expertise back from the battlefield, and from wherever they've been deployed in the past. It makes a very good team to have the military and civilians there.

I said I'd show you where we're located (figure 4). This is sort of a snapshot. I have people everywhere you see these arrows pointing. Clearly we're heavily located in the United States, but I also point out Alaska, Japan, Okinawa, Guam. Wherever we have a combatant commander, one of the commanders in chief (CINCs), I have a field office, and the job of that field office is to be there day in and day out to be that CINC's voice and that interface back into what's a very complex organization. They have to make sure that the CINC's problems are well understood, and that they draw on the available resources—for example, that large number of engineers I have. I will send them out to a location to work on a particular problem for a CINC.

Some time back, right after Desert Storm, this vision was articulated because, in spite of all our technology, we ran into a lot of problems in providing information to the warfighters during the Desert Storm activity, just as we did in Grenada, when we had interoperability problems with the radios between the Army and the Marine Corps (figure 5). So one of the visions we took out of this defines what we want to do. For every warfighter—whether on an aircraft carrier, on the ground, or running the air war—we want this capability of a fused, real time, and true picture of the battlespace. That mission, or that statement, drove us to develop the GCCS, which is sort of the instantiation of it. I'll get into that a little bit when we talk about that system.

That was right after the war. Lately, the Joint Chiefs have come up with what they call "Joint Vision 2010" (figure 6), which is trying to capture what we visualize warfare will be like around the 2010 timeframe, and

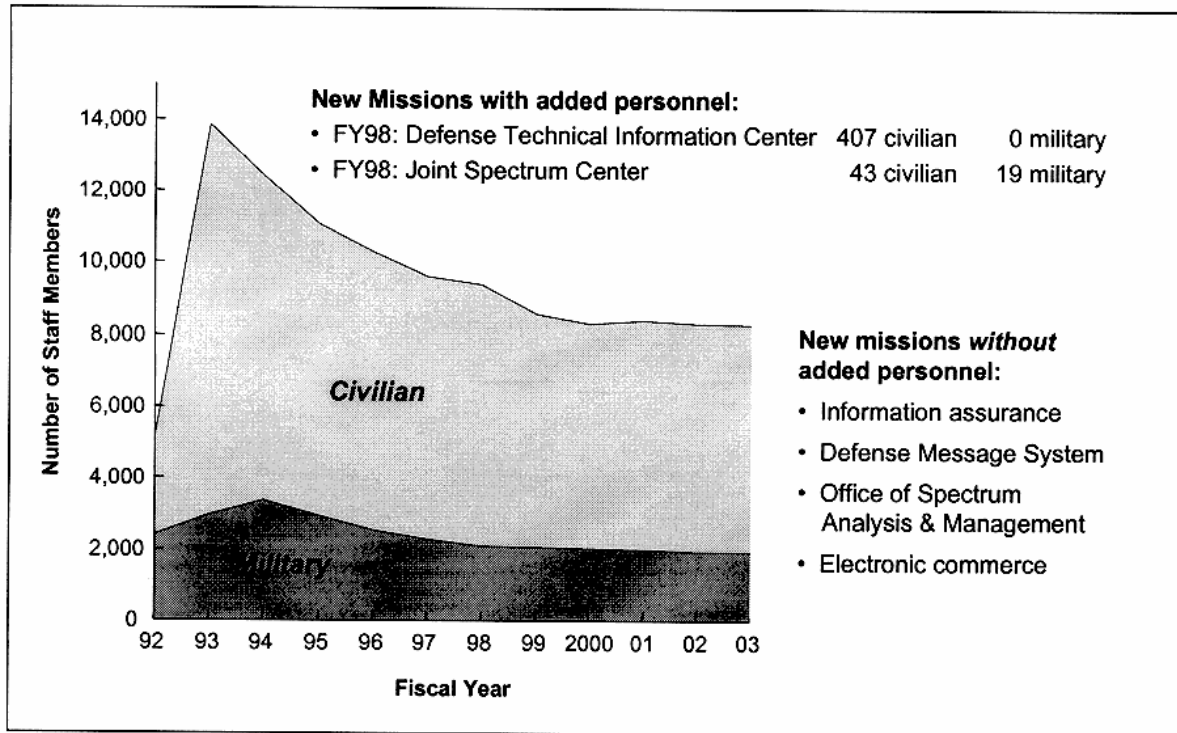


Figure 3

DISA End Strength: Fiscal Year 1992–Fiscal Year 2003

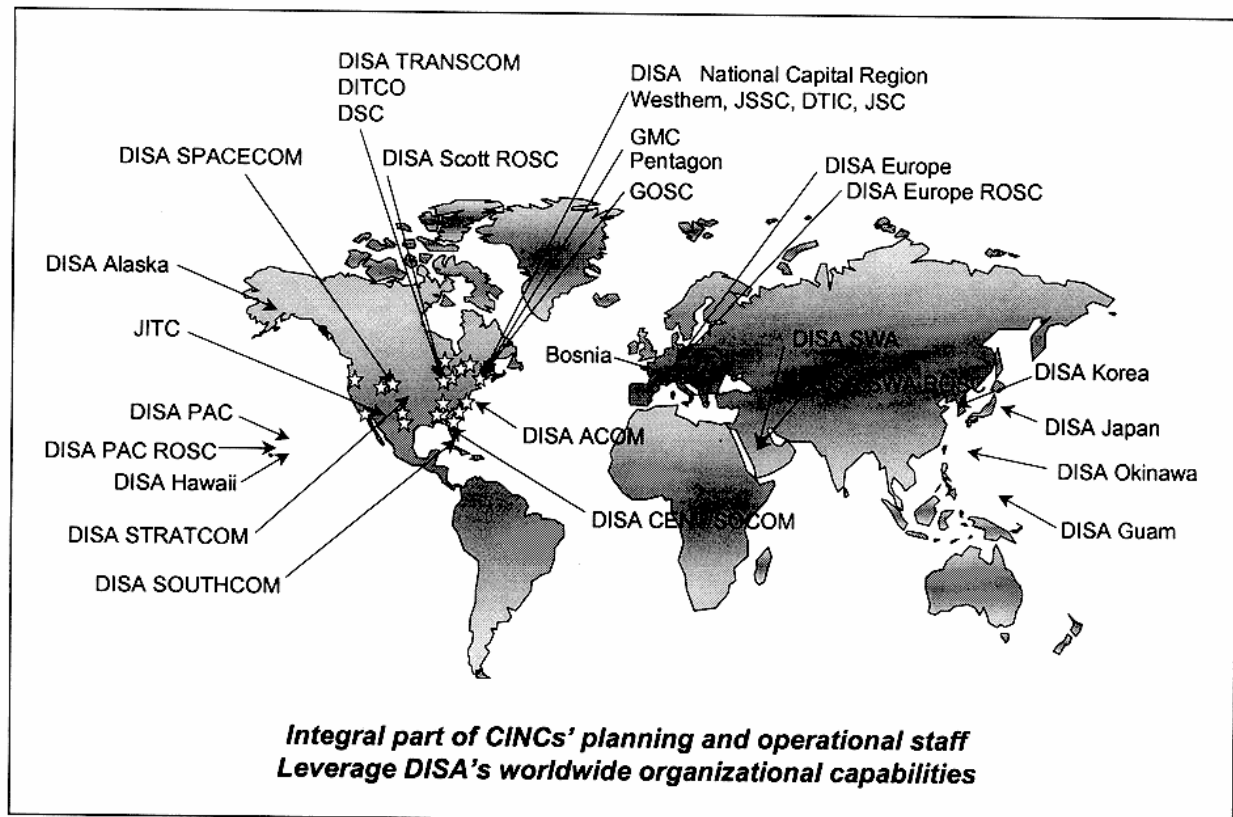
to give all of us a direction in which to head—everybody developing weapons systems, developing planes, and, in my case, developing command and control systems. That's what Joint Vision 2010 is. These are operational concepts. I would submit to you that you will see more precision and engagement on CNN tonight.¹ We're far better than we were during the Desert Storm war in that particular area, and we're going to be far better in 2010.

But this is the idea: we've taken each one of these, and what I've tried to do is develop a system that supports a particular theme; for example, when we focus on logistics, that's where we get into this GCSS I talk about. You can see some of the acronyms that we've got over here. For command and control, there's the GCCS. This is the Defense Information System Network (DISN), the transport layer that Pete put in, and he's go-

ing to talk about that. The Defense Message System (DMS) provides interoperability with our allies, which is extremely important. That's one of the areas where we, in fact, come to a level where we can interchange messaging with our allies, following allied communications procedures.

INFOSEC has been a growth industry. I would never have guessed the amount of resources I've had to put on it, or the number of people. It sort of parallels the growth in the Internet. We've had the same type of explosive growth inside the Defense Department, only a lot of that growth we put behind security classification and encryption and so forth. But we're trying to capture all the problems of the growth of the Internet and the power of the Internet for the warfighter. The ability to exchange information that we have now is great, but guess what! It also brought with it a whole host of problems we hadn't considered, because it sort of got out in front of us. That's why you read in the press now that the Department of Defense is working hard on information assurance, and

¹ This presentation was given on March 25, 1999, one day after the start of the NATO air attacks in Yugoslavia.



☆ = Combat information support processing
 DITCO = Defense Information Technology Contracting Office
 GMC = Global Management Center
 GOSC = global operations and security center

JITC = Joint Interop/Test Command
 JSSC = Joint Staff Support Center
 ROSC = regional operations and security center
 SWA = Southwest Asia

Figure 4
DISA Global Presence

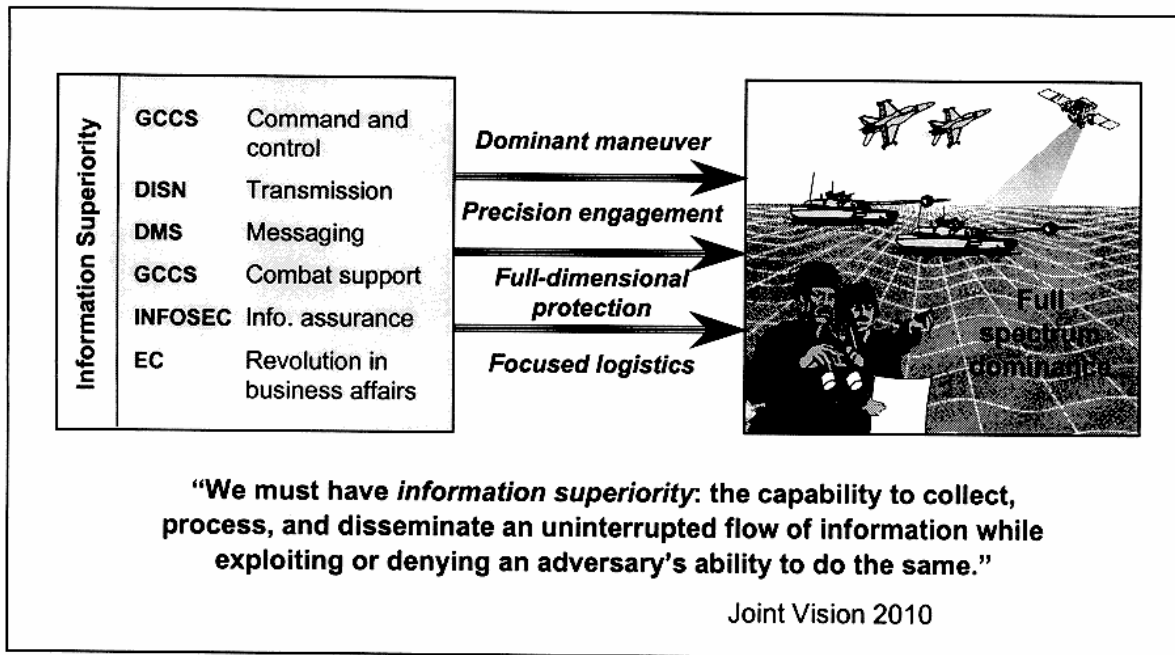
The warrior needs a fused, real-time, true picture of the battlespace and the ability to order, respond, and coordinate vertically and horizontally to the degree necessary to prosecute the mission in that battlespace.

Figure 5
C⁴I for the Warrior: The Vision

we're spending a lot of dollars on it: because it caught us by surprise, just as the Internet growth, I think, caught everybody else by surprise. We're making a lot of progress, and we'll talk about that to the extent you're inter-

ested. We just formed the Joint Task Force for Computer Network Defense (JTF-CND). My vice director is a two-star Air Force general, and he is the commander of that organization. He reports to the CINC at SPACECOM and to the SECDEF under that hat. So there are a lot of areas we can take off, but I think it's important we do an overview like this to try to pique your interest.


Let's get into the battlefield pull (figure 7). In the final analysis, everything we do in the agency really is directed to supporting the JTF or whatever young Americans we send out, and supporting our allies, when we go into harm's way. We try to learn from the past. We truly do, in spite of what some of the press would have you believe. We do critique ourselves, and we do know, for example, that in Desert Storm the air tasking order

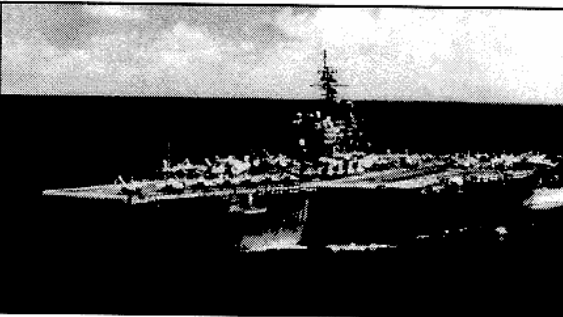


EC = electronic commerce

Figure 6
DISA Programs Support Joint Vision 2010

We put more communications in theater in 90 days than we put in Europe in 40 years...but we had problems with imagery ATO dissemination.





Containing daily attack requirements for all coalition aircraft, the ATO could only be transmitted through Air Force channels.

It therefore became necessary to print the ATO every day and fly it to every aircraft carrier.

Figure 7
Desert Shield/Desert Storm: Lessons Learned

(ATO) was a big problem. That was just one example where it was sort of internal to the

Air Force. But, guess what! We have Army helicopters flying. We had a tragic accident

because they weren't in the ATO.² We've got the Navy aircraft carriers that provide a lot of the air-to-air type aircraft, and we all need to be able to get the ATO. That came out of Desert Storm, and now, of course, we can all get it.

But guess what! We also had every service developing their own ATO, which meant they weren't interoperable. We solved the transport problem initially, but then the next problem hit us, which is that the Navy doesn't use the Air Force ATO. The Army doesn't use either one. That's where we've been trying to work the interoperability piece, and that's where the GCCS comes in. There we've agreed that the Air Force will do the tasking order, the Navy and the Army will do some other applications, and we're going to share those things because we do not fight as independent services anymore, ever, as we see the future.

The other problem we saw in Desert Storm was the ability to get secondary imagery out (figure 8). We were ill prepared at that time to do anything that required large-bandwidth pipes. If we had tried to take the imagery and put it on the tactical communications systems, we'd have flooded them.

"The major problem was the insatiable demand for the imagery used in targeting information, bomb-damage assessment, reconnaissance.... Root of the problem was the lack of effective alignment between the sensors deployed by each of the services and the communications pathways needed to deliver this information to those who needed it."

Alan Campen,
The First Information War

Figure 8

Desert Storm: Need for Information

There just wouldn't have been any room for anything else. So, what we've been doing since that time is looking at technology where we get into global broadcast, which allows us to send a very large pipe of information into a

feeder to a receiver anywhere. It's much like TV. You have a receiver out there. You can receive the pipe, and now we're working the issues of how you load that pipe. It's 24 megabits per second, and that's a big pipe. That's something we have now that we didn't have during Desert Storm. We've been using the prototype stage in Bosnia very successfully. In fact, we're deploying it to the Pacific and into Europe over the next year.

I'm going to let Pete take over and talk to you a little about what we're trying to do at this transport layer and to give you a little perspective on what we've done. This is an example. I'm not going to go into this much detail on the other ones, but I think it's a good case study on how we go about this.

Paulson: Largely as a result of a lot of the problems General Kelley talked about, there were interoperability problems and there were expense problems associated with every time we went out on a military maneuver or war-fighting mission. Whether it was things like the *Pueblo*, Grenada, Panama, or Southwest Asia, we found problems associated with horrendous expense and a total lack of interoperability. A lot of disparate networks were being sent to the theater, leaving the theater commander to say, "What am I supposed to do about this stuff?" He couldn't integrate it; he couldn't interoperate it. As a result of that, in the early 1990s, there were a lot of policy implementations put out, as well as some requirements documents put out by the Joint Staff.

What I would like to highlight are two primary documents that really drive us on the DISN (figure 9). They are the JMNS, the Joint Mission Needs Statement, and the JCRD, the Joint Capstone Requirements Document. What basically these documents said was, "We're going to put an end to this madness." They wanted us to go out and build a global network that is a private network for DOD, and it had to have several characteristics. It had to be protected. In other words, we want protection from information warfare attacks, i.e., hackers getting into the network. It had to be broadband. The JMNS and the JCRD recognized then that with this explosive expansion of data we need broadband pipes. We had to have positive control.

² A reference to the "friendly fire" shootdown of two Army helicopters in Iraq.

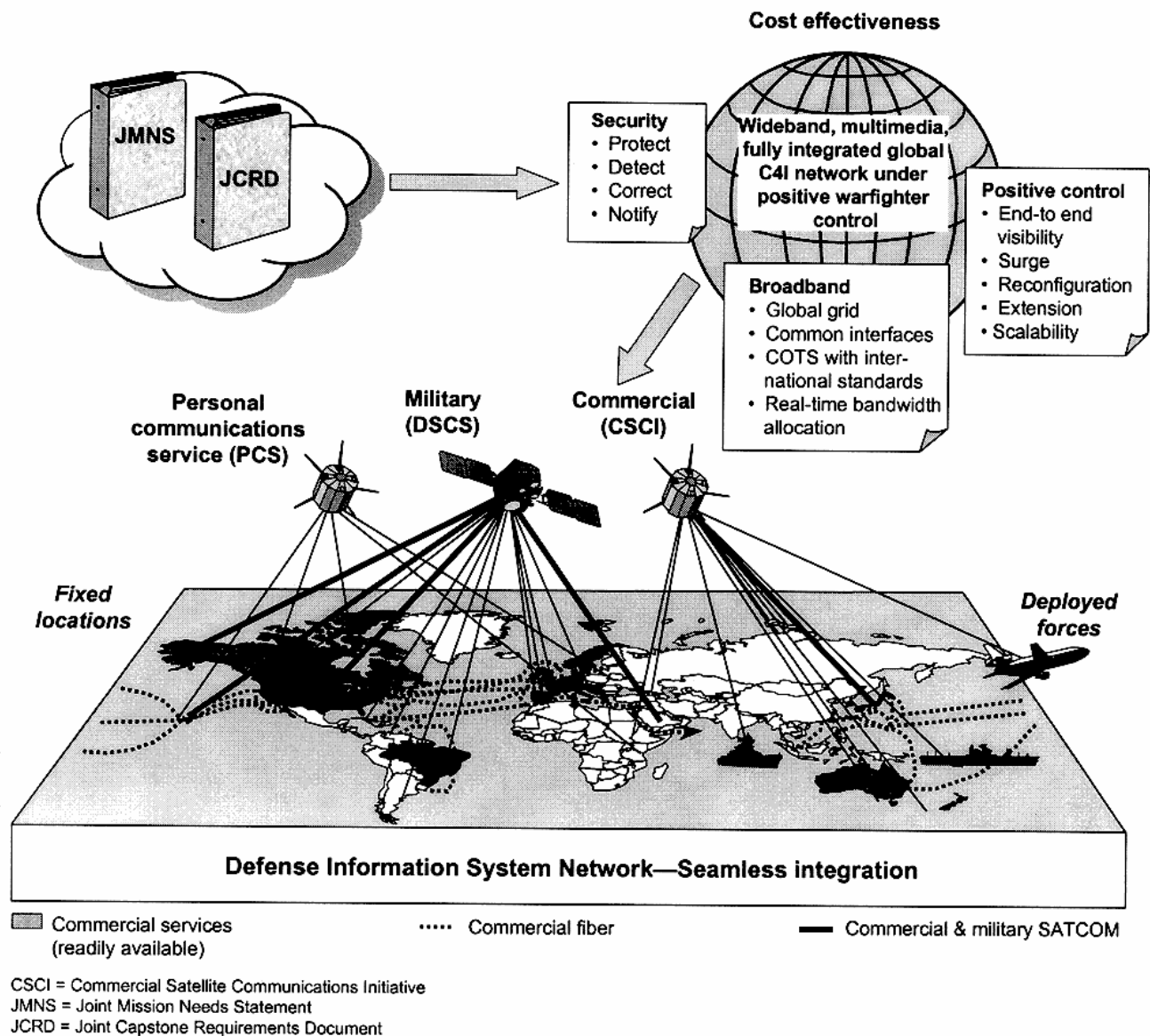


Figure 9
DISN 2000 Requirements

What positive control means is that we in the Department of Defense want to be masters of our own destiny. We do not want to be beholden to the civilian-run companies that would impose their own management controls in times of crisis. Back in the old days, they used to call these controls the "Mother's Day syndrome," because that was when they had the peak volume on telephone calls. They would intentionally go into the network and block out certain areas of the country, or every tenth call automatically was thrown out. We did not want those kind of manage-

ment controls imposed on the Defense Department.

Last but not least, the documents said, "You've got to make this cost effective. In other words, we can't pay an arm and a leg for this. You have to show us that this is worth investing in." So, as a result, the end thing that they wanted us to produce was this terrestrial infrastructure, linked and augmented by a lot of different satellite infrastructure. Whether that be government owned, Defense Department owned, or in any way commercially provided, the chal-

challenge was now to build that infrastructure and link it to space so that we have the ability to project to any theater of war we go into.

Let me talk about the cost effectiveness of what we wanted to do (figure 10). Before this, typically we bought down at the low end of the spectrum. I'm not sure how familiar you are with communications technology. A T-1 is about 1.5 megabits per second, and we go up here to OC-12 at 620 megabits. What we've shown here is the relative cost per kilobit of buying it in small bandwidth pieces. The notion was that if we could combine all the Defense Department's requirements into a larger pipe, we could now operate up at the

OC-3 end of the spectrum, and our unit cost per kilobit would dramatically decrease. You can see relative orders of magnitude difference in those prices.

Oettinger: Isn't that antithetical to the notion of assurance? Is this metaphorically one pipe, or price-wise one pipe, or literally one pipe?

Paulson: It's a metaphor. We're not going to have just one pipe, but we're going to have multiple OC-12s. I'll show you a couple of examples in there, with robustness and all-around capability and those kinds of things.

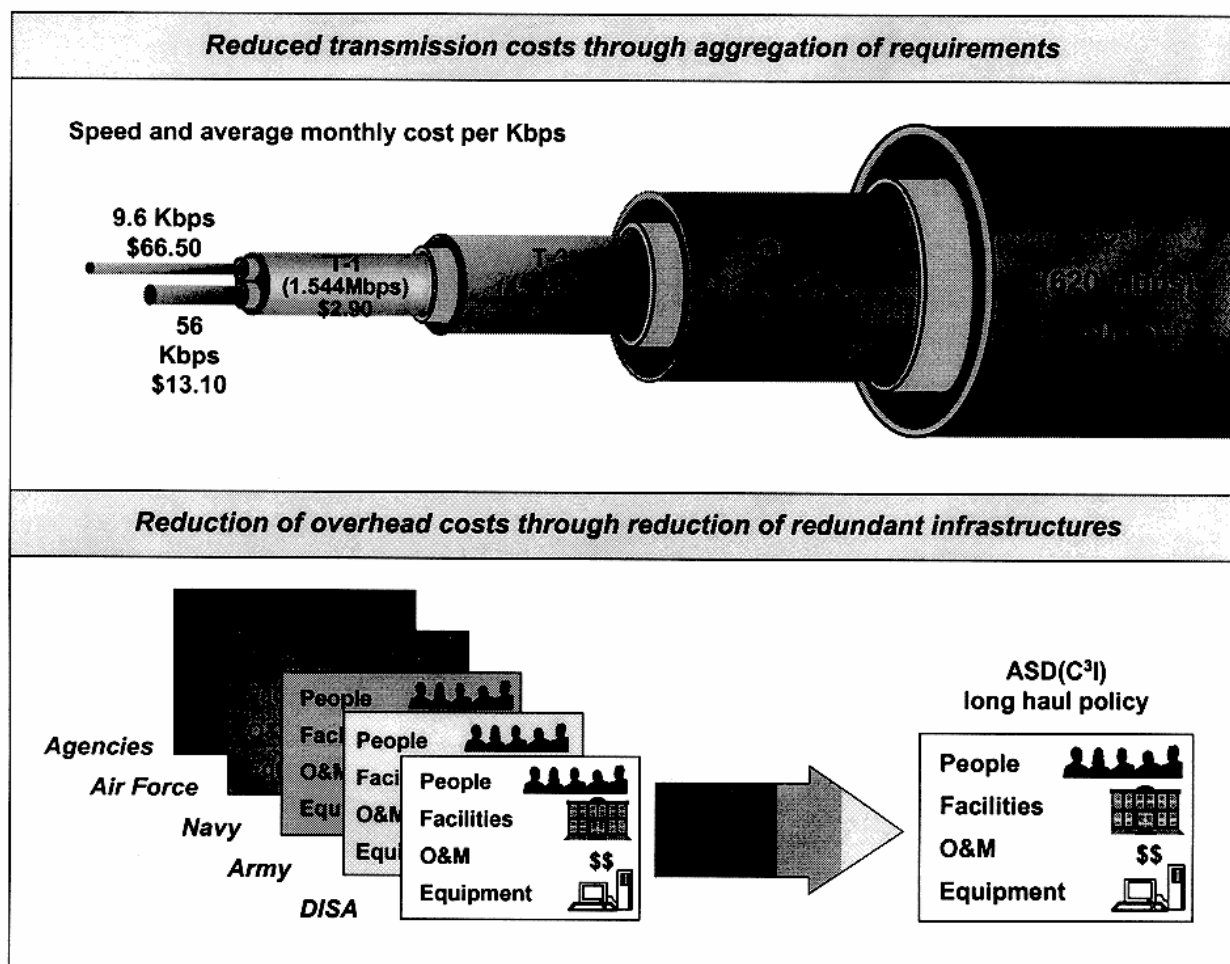


Figure 10
Economies of Scale

Kelley: We're worried about cables being cut, especially after Italy.³

Oettinger: If we have to take that literally, it's going from the frying pan into the fire, but if it's metaphorical, I'll shut up.

Paulson: The other dimension of this economy was that prior to this the agencies and each of the services went out and kind of created their own global networks. So we had redundancy all over the world, but we didn't have interoperability, and we certainly didn't have economies. We felt that if we could

combine this into a somewhat single infrastructure we could reduce the people, the facilities, the O&M (operations and maintenance) costs, and the equipment tails associated with a lot of disparate networks.

We started in CONUS (figure 11). That was our first task. We got the requirements from the Joint Staff in 1995. We awarded the contracts in late 1996/early 1997. For those of you who have ever been associated with the Defense Department, to be able to do that in two years or two-and-a-half years is warp speed. That is very, very quick.

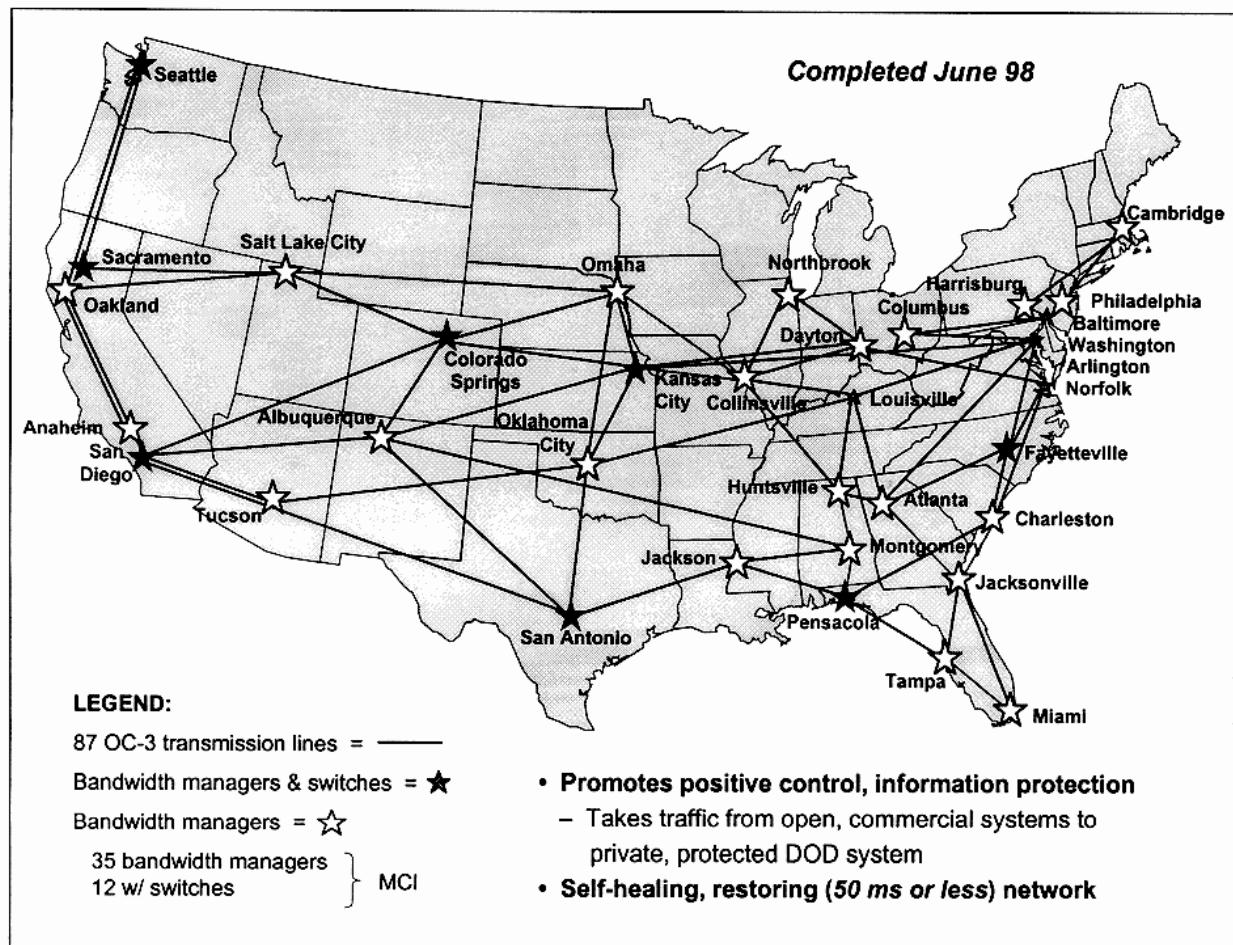


Figure 11
DISN 2000 CONUS: SONET Backbone

³ A reference to the cable car disaster in Cavalese, Italy, on February 3, 1998.

This is the backbone component only, and we had this completely installed by June 1998. Here's whom we contracted with to provide that. Basically, AT&T provides all the lines; MCI provides all the stars. Those stars represent our switching centers. Those are our node centers on our backbone. Those are purely government-only switches. We do not allow any interface into the commercial infrastructure at those points. We have both what we call bandwidth managers, which handle just the transmission, plus our voice switches at 12 of those 35 locations.

From those 35 node centers, what we do is extend out to about 600 geographic locations within CONUS (figure 12). You can see the number of circuits and trunks that we had to transition from the old to the new system. We did this in little less than a year. This is probably the largest nonpublic carrier transition in history. It was a very intensive effort, very high anxiety, and there were a lot of problems. But, it was very successful.

If you look back, this is kind of what we looked like before (figure 13). We had circuits just running everywhere. There was no configuration management; nobody really knew what was going on. The right side of the slide shows what we currently have on the backbone. From a cost point of view, we were able to replace that old stuff with the new stuff at about half the cost. We were paid back for our transition costs and everything in less than a year. It was a very, very wise investment.

Restoration time. In the old days, if we had one of these circuits cut, we knew that literally it would be out for hours, if not days, depending on where it was.

Positive control. We had no control over this; I mean, el zero. Right now, we control this entire backbone from a place called Scott Air Force Base. That is our facility where the orders are issued to MCI and to AT&T.

Surge. Previously, we had no surge capacity. Here we run about 20 percent of all

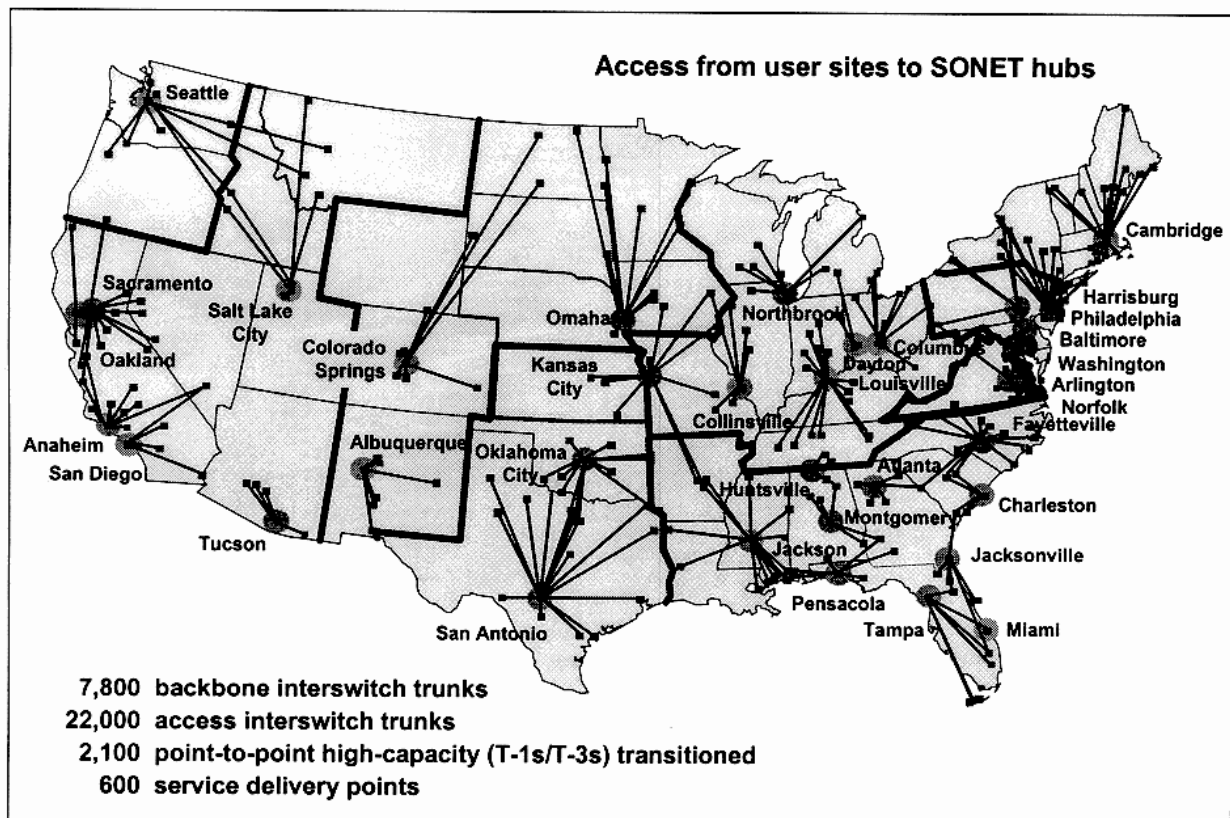


Figure 12
 DISN 2000 CONUS: Regional Access

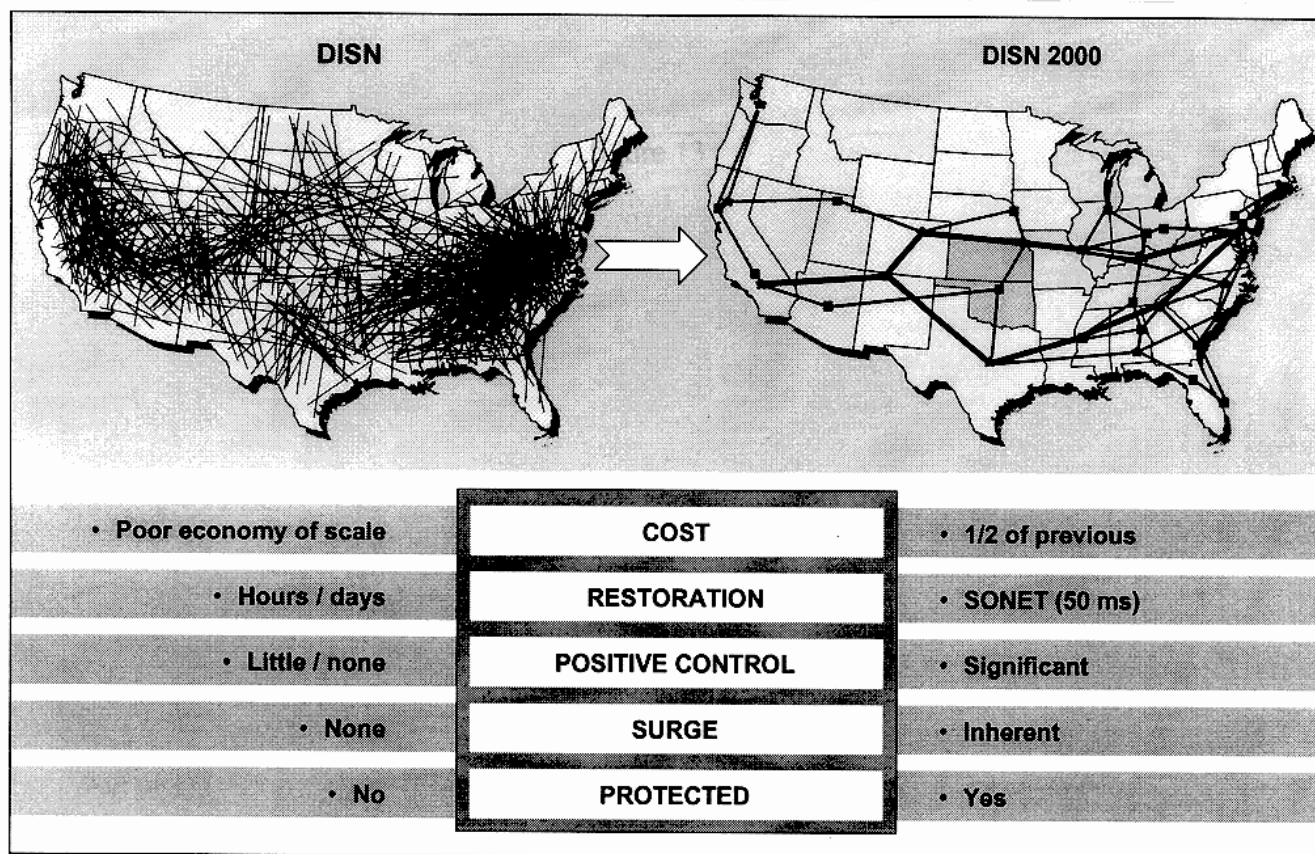


Figure 13
DISN 2000 CONUS Transition

that capacity as spare. That gives us the capability to respond immediately to urgent requirements. And, of course, it's protected, where the other one was not.

Oettinger: You emphasized "owned" switches, but were silent on the links between switches. Again, what's metaphor and what's real here in terms of whose facilities these are?

Paulson: Obviously, the bandwidth is provided through AT&T facilities, but we think the susceptibility from an information attack point of view is very likely to occur at the switching centers. That's the weakness we wanted to protect. The alternative was that we could have gone ahead and bought our own fiber, buried it, constructed it, and built these all-government-owned networks. When you start to do that, you're looking at costs that are just astronomical. This transition probably cost us somewhere in the neighborhood

of \$70 million or \$80 million. Had we elected to construct that with government-owned fiber, it probably would have been \$8 billion to \$10 billion. So obviously, the economics said, "Okay, minimize your risks where you can, but you can't totally shut the door." We think that we pretty well shut the door against outsiders in terms of our switching centers. You're always going to be susceptible to insiders.

Let me mention one other thing here. What the old DISN really gave you was a lot of redundancy. DISN 2000 apparently doesn't give a lot of redundancy. So if you have a cable cut, you think that you'd lose this whole thing. One of the things that permitted us to do this is that we've employed a new technology that's called SONET ring technology. If we have a cut somewhere, we lose nothing. Restoration time is 50 milliseconds, because it's what we call a counter-rotating ring. It just goes the other way. That was one of the very important aspects that permitted us to do that. Had it not been for

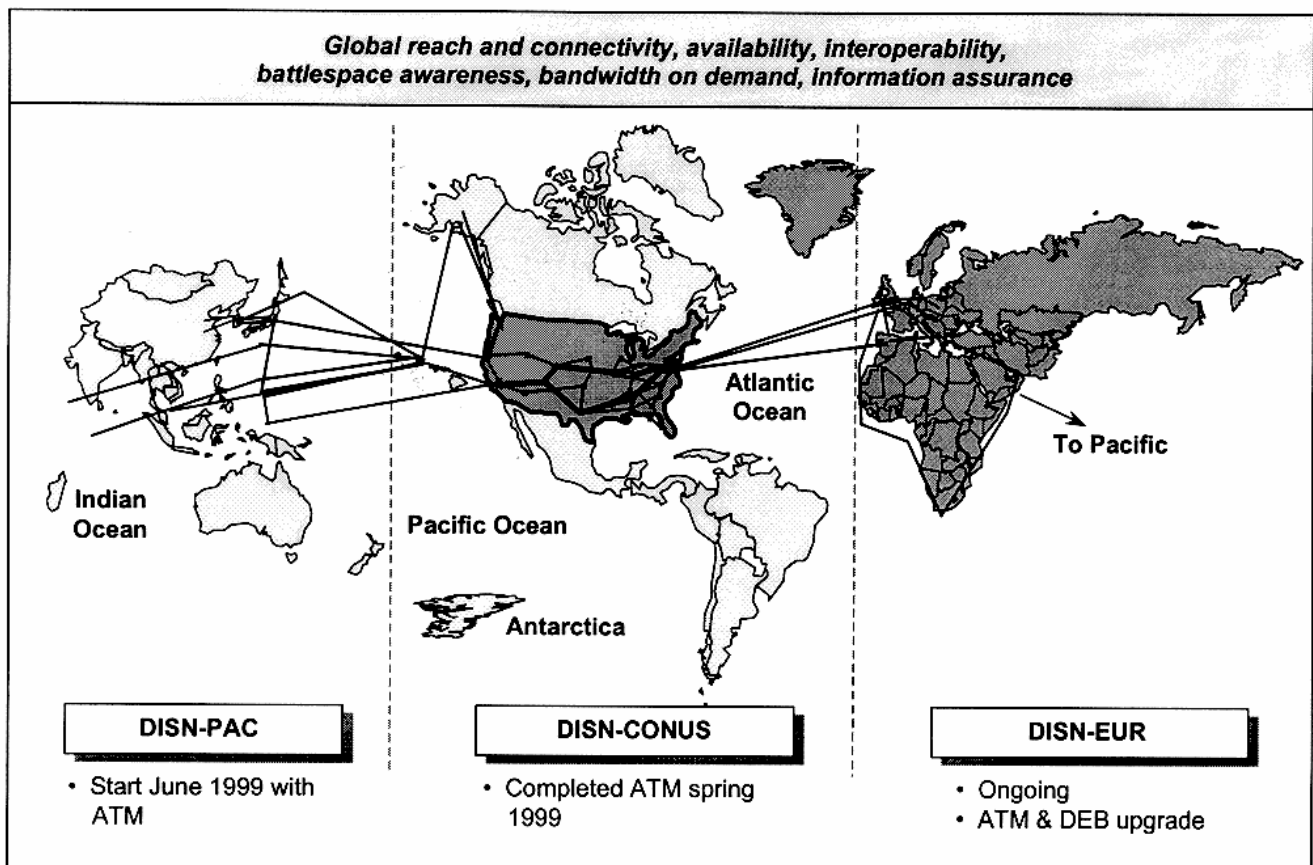
that technology, we would have been foolish to erect this.

Student: We've already been discussing a lot of this, but there is an issue about the interface between civilian business and the government and the sensitive area it represents. When you talk about positive control, could you say a little bit more about it? Is it a case where physically the contractors control the assets, but all policy decisions are yours?

Paulson: It's much more the physical piece than it is the policy piece. Let me give you an example. If we detect an information attack, let's say coming from the West Coast, that is now encompassing everything, we can shut the West Coast component off immediately. That is our call. That is our decision. We can issue orders to those bandwidth managers that say, "Terminate those links right now,"

and so, we can protect parts of the network. If we have massive failures elsewhere, and let's say we want to give priority to the users in the southeastern part of the country because they are the ones who are in most need of it, or they are given the highest priority, we can shut the rest of these people off. So we are, in fact, masters of our own destiny from the Defense Department's point of view. It's not so much a policy issue as it is the physical control of that network.

We're taking that same general philosophy that I told you about, which we implemented in CONUS, and we're applying that to the Pacific and to Europe (figure 14). In Europe right now, that is ongoing. We're kind of doing that ourselves, as the Department of Defense, as opposed to going out on a massive contract. In PAC, we will go on contract. This will be a 10-year contract worth about \$4 billion. We have just received



DEB = digital ethernet backbone

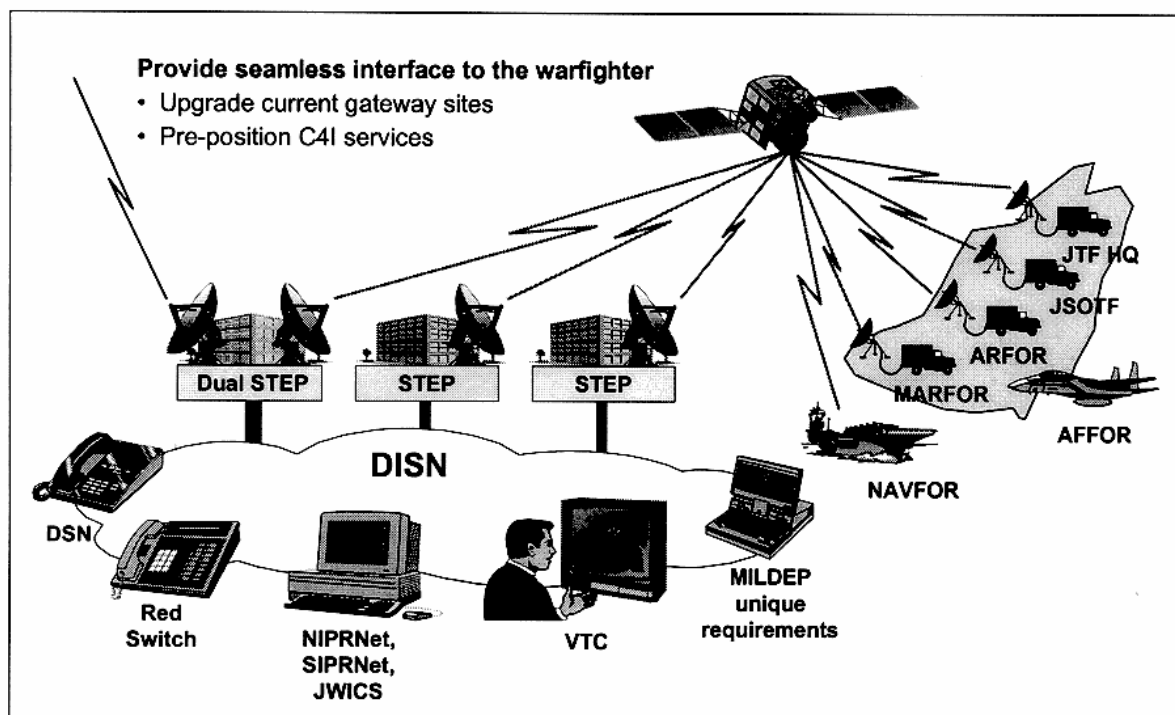
Figure 14
DISN 2000 Status: Foundation of Defense Global Grid

the proposals. We expect to award that in May, and we will probably get ramped up and start physically making cuts in the existing network over in the Pacific, which is very much like the original DISN in CONUS that I showed in the previous slide, but maybe on a smaller scale, and we will start a transition effort in PAC.

We're going to bring on our own asynchronous transfer mode (ATM) overlay. Am I talking Greek to everybody? ATM is new technology. We have already put down the node centers. We've ordered the equipment from Ford. We will probably have that totally installed here within the next, I would say, 60 to 90 days. We're already starting to lay down an ATM in Europe. This transition I talk about in the Pacific will be done with ATM.

Now that we have this wonderful terrestrial infrastructure, the issue becomes how do we now support that warfighter as he deploys (figure 15)? If we move into Kosovo, how do we get to those guys? I don't have those

big pipes going into Kosovo, or going into Nicaragua, or wherever. What we use is called the STEP, the Standardized Tactical Entry Point. This is where we want to put the interface between the tactical guy out there and all that wealth of information that he needs in the permanent infrastructure. His home station is logistics, infrastructure, all of those things. This is what we typically provide. DSN is our voice: our privately owned voice networks in the Department of Defense. Red Switch is the same thing, except it's for, let me say, the high-powered users. It is classified at the Top Secret (TS) level; they can talk TS on it. NIPRNet (Nonsecure Internet Protocol Router Network) and SIPRNet (Secure Internet Protocol Router Network) are the mainstays of our data networks and our information processing routers. SIPRNet is at the Secret level. Obviously VTC (video teleconferencing) is becoming more and more important as a command and control means, not just a nice-to-have thing. There are also some unique requirements.



DISN = Defense Information Systems Network
 DSN = Defense Systems Network
 JSOTF = Joint special operations task force

JWICS = Joint Worldwide Intelligence Communications System
 VTC = video teleconferencing

Figure 15
Standardized Tactical Entry Point: STEP's Goal

We connect the DISN through these STEP sites. Basically, they are satellite terminals, and we beam those signals up and send them into whatever part of the world where that force is employed.

Here's our problem: the satellite capability to project into the theater of war (figure 16). Right now, if we have four STEP sites available to support that theater of war, which is the most anyplace on the globe can get, our maximum throughput is about 45 megabits. What the Joint Staff told us three years ago was that in a major theater war—not a Kosovo or a Bosnia, but a major theater war like Southwest Asia—what we need is 102 megabits. Currently we're limited to the frequency band in the satellites that the government owns, the DSCS (Defense Satellite Communication System) satellites, and that's the X-band. We need to take some of those STEP sites and expand those so that we can do the Ka-, the UHF-, the C-, and the Ku-bands, which are the commercial bands. This is a concept that we currently have in front of

the Joint Requirements Oversight Council, going over to the Joint Staff, to say that if we want to support the warfighter and connect him back to his CONUS infrastructure, we need to have this funded. Roughly, this would cost us probably anywhere from \$100 million to \$300 million depending on how the requirement finally comes down.

In summary, that satellite capability is really essential for us to project that DISN infrastructure into the theater of operations and to give the warfighter seamless connectivity back to CONUS (figure 17). That is our most important principle. We know that we're going to have to augment that with commercial space. The Defense Department does not have the dollars to be able to put that kind of investment into space for a major theater war. So reliance on commercial industry is absolutely essential. Optimization of space and terrestrial is always a challenge. How are we going to do that? "Go anywhere, go anytime" is what we want to do. I think I'm back over to you, sir.

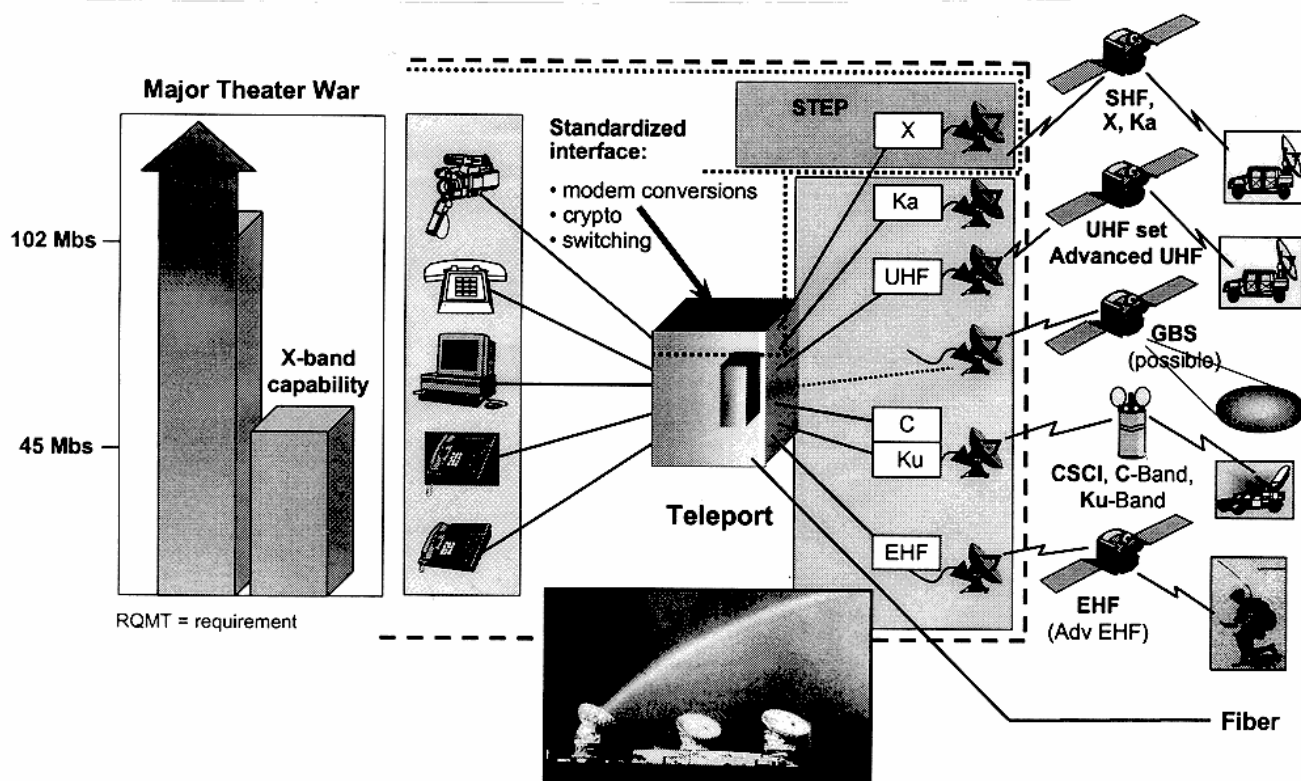


Figure 16
DOD Teleport Configuration

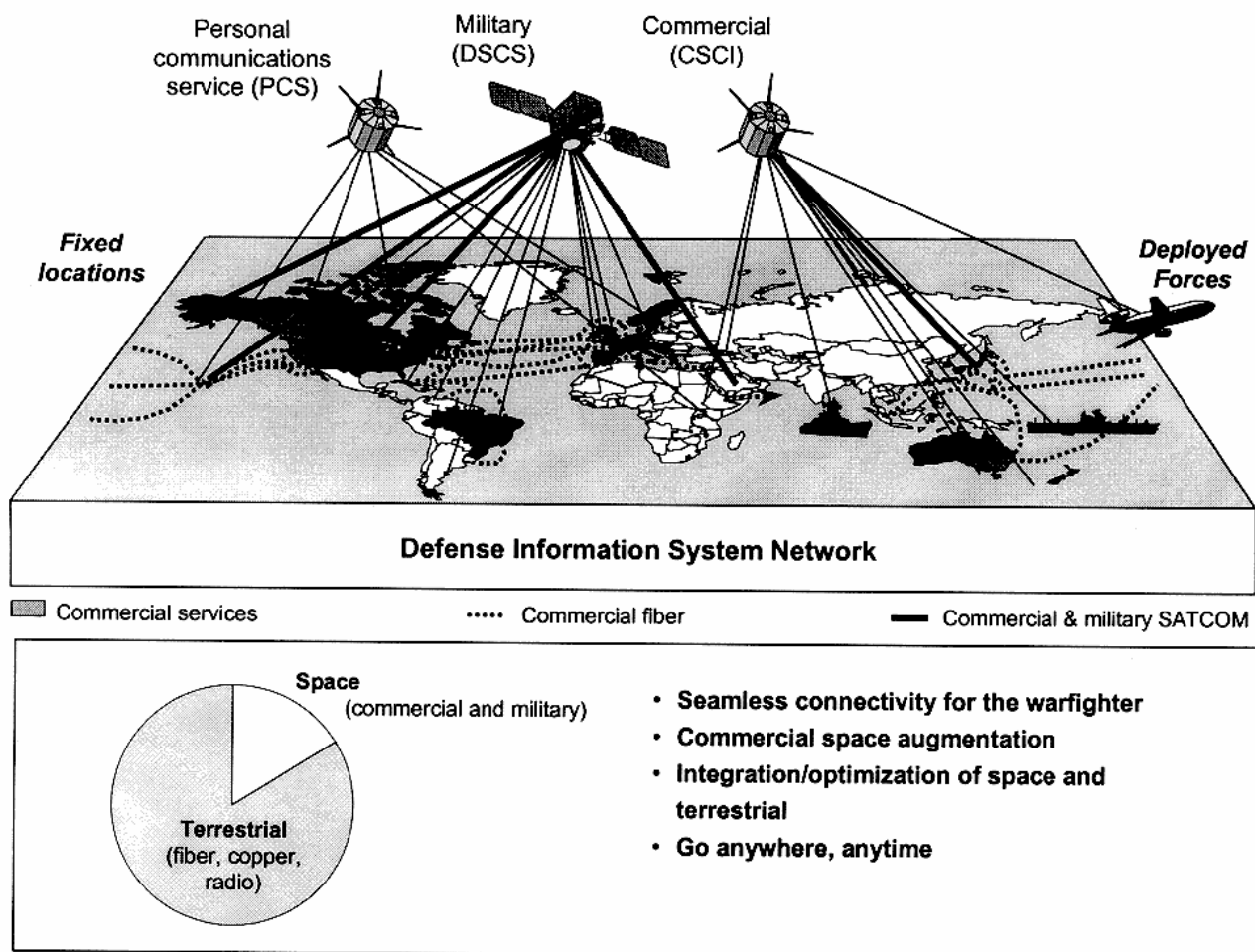


Figure 17
Objective: DISN 2000

Kelley: To reiterate what Pete said about VTC becoming a command and control tool, General Byrnes is the first cavalry division commander in Bosnia right now (figure 18). He's got one brigade of his division with him, and the next brigade is, in fact, getting ready to go over there. They're doing all the planning via VTC with him in Bosnia and his headquarters back at Fort Hood, Texas. Without this capability, it would be endless messages going back and forth ... and misunderstandings. But this almost allows him to be a virtual commander, because they're executing one mission while he's planning the other one, and he is in control of both actions. It's technology that's letting him do that. Some people ask, "Is that good?" Yes, it is, because he's the guy in Bosnia who's got

all the lessons learned right now. He knows what this next brigade should do to make it better for them for when they come in there.

Student: I was wondering whether VTC is actually a real-time tool. For command and control, on demand is really what you want, and the bandwidth requirements for a VTC sort of preclude that in my view. Is that still something that is being wrestled with?

Kelley: Yes, the bandwidth is still being wrestled with, but we're looking at the situation. At the major headquarters, when we're doing peacekeeping operations like this, we routinely put in VTC. Remember the discussion on space we just had? Where we don't have enough capacity in the military, from a

Video teleconferencing has become a command and control tool

MG Kevin Byrnes commands one brigade of his 1st Cavalry Division in theater with the remainder at Fort Hood. He relies heavily on VTC to exercise command over this split base operation. Conferences are scheduled almost every evening. In addition, for morale and welfare, soldiers have access to IP video back to their home station.

Large impact on bandwidth requirements

Figure 18

Supporting the Warfighter: Bosnia

peacekeeping standpoint, or for a humanitarian operation, we supplement it with commercial satellite capability. We're very concerned. We're not trying to say it's going down to a very low level in the battlefield right now, but the major headquarters that are orchestrating an operation and the people responsible for planning now depend on it, and they, in fact, do have it.

Now, let's talk about an interesting issue here, folks (figure 19). The way the Department of Defense is organized, we have a whole host of functions and systems. Every service has a personnel system. They're all different. Everybody has a logistics function, a finance function, a medical function, a maintenance function, and on and on. These functions have the money and the responsibility to develop programs to optimize their activities. Do you see where I'm going with this? Then you get out of the function and you come over to the services. Each service has these functions, but the Air Force function for personnel is very different from the one in the Navy. The folks on the left and in the middle of the slide have the money in our system. This guy on the right has very few dollars, but guess what? He has a very big responsibility. General Wes Clark is the guy over there doing the Kosovo thing right now. The question then becomes: How do we get these other guys, who are great Americans, to understand fully that what they do has to optimize his agenda, not theirs? That is a fundamental shift we have to come to grips with.

This is why every time we go to a Desert Storm, we get in there and we have problems. We know about them and we say we're going to fix them, but the power of the dollar and of these stovepipes here is intense, and the further we get away from Desert Storm, the fewer people we have who were on active duty at the time and remember what the problems were. And so, guess what happens? We start diverging again, and for very good reasons. The logistics guy in the Navy figures out that he can do something that's really swift. He does it. The next thing you know, we float another JTF to go overseas, and guess what? Here comes one of those stovepipe systems that doesn't interoperate. It goes back to Pete's comment. So, if interoperability is really important to us, we're going to have to get really tough on the left side of the equation.

Oettinger: Tell me if I'm off the wall or not, but I want to make sure the class understands that interoperability is not only a technical problem. You'll find in the record of the seminar (and this is germane to Kosovo as a NATO operation) 20 years of argument over NATO interoperability.⁴ The issues that General Kelley describes here in the American context recur magnified in the NATO environment. You find over and over again on the one hand the pressure of the commander, whoever it might be, to have some kind of coherence, and the national government's insistence on maintaining an indigenous industry and looking at the problem from an economic point of view. That says, "We want it manufactured by Siemens or Thompson or whoever," and then the interoperability is only secondary. So the question of why this is a hard problem, and why General Kelley is emphasizing it so strongly, is not truly a technical problem. It is one of the messiest financial and political problems there is in this kind of area. Is that a reasonable statement?

Kelley: Absolutely. This chart (figure 19) oversimplifies it. I would put brackets around the function and service columns and then

⁴ See, for example, Barry M. Horowitz, "The Emergence of Data Systems: Cost and Technical Change in Military Systems," in seminar proceedings, 1993.

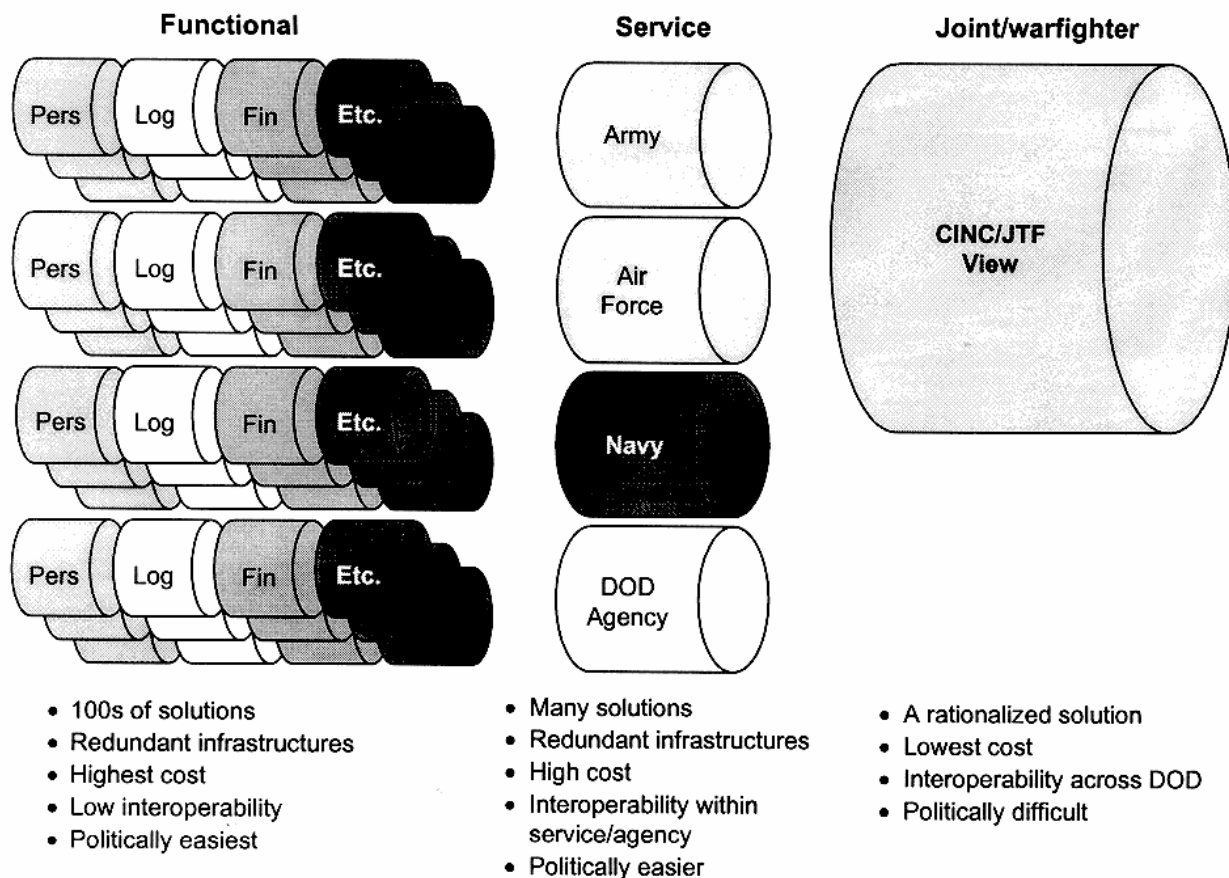


Figure 19

Choosing the Level of Optimization for the Enterprise

you pick the exponent and put it up there. This is an exponential problem. It's really difficult.

Student: Last week I talked with the German defense minister, and because this was an obvious issue, I asked him how he felt about the whole status of interoperability between NATO forces and U.S. forces. He said, "Oh, that's not a problem!"

Kelley: It's a problem. Now, let me suggest a thesis to you why it's sort of a problem now, but it wasn't so bad a few years ago when the Berlin Wall was up. How many times had we deployed military forces before 1989 in the types of things we've been doing since 1989? In other words, Russia held us stalemated and we were in a sort of status quo type thing. So we were ready to fight each other, but the visibility of these interop-

erability things didn't come up that often because we weren't deploying that much, and we weren't working in a coalition that much. But all of a sudden, we've got a very activist policy now in this brave new world, and the problem becomes visible every time we throw a JTF together. So the theory of visibility says it's going to get tougher before it gets better.

Having said that, the warfighters in the United States—really every CINC—are not dumb individuals. They understand this problem fully, and they're doing everything they can. I see a shift going on even as we speak. Without question, the power in the military is shifting to the warfighting CINCs. It used to be, before Goldwater-Nichols, that the chiefs of staff or the chief of naval operations were extremely powerful. Not only did they have resources, but they could also allocate and say what you got, when you got it, and so forth. Not anymore! As a result of

Goldwater-Nichols, that all comes now from the Joint Staff playing with the SECDEF. I think that as they solve more of the service problems they are going to go after the money and a lot of the functional problems that we're talking about, and before you know it, there's going to be a joint process over on the left side of the chart also. We just haven't gotten to them yet.

Student: What about in a broader government sense, where we're having this situation in Kosovo now? Obviously it's a military-NATO interoperability kind of issue, but there are other players. There is the President of the United States; there's the Department of State; there's the CIA.

Kelley: There are the nongovernmental organizations, like the Red Cross.

Student: How does this now work? Are there trends toward improvement in abilities for those organizations to feed into what's going on in the military side?

Kelley: As a matter of policy, a lot of the nongovernmental organizations do not want to be associated with us, and rightly so, because of the credibility they have to have in the country when we leave. So we're very careful how we do that. But we've got to distinguish between operations. If it's a friendly type of situation where we've been called in, we can obviously work more closely and more openly with them. If it's not friendly, then we don't want to taint their efforts later, after we've done what we're supposed to do there. So there is no one answer for you. The answer is, "It depends on what the situation is."

Student: I guess my question is more pointed toward governmental entities that play an active role.

Kelley: Haiti is a good example. Before we did the Haiti exercise, we met with every element of the government, and the CINC chaired the meeting. We brought in the Justice Department, the whole crew, because once you shift toward a military option, then the other aspects of the government move in

with the CINC to see where they can help. Police was a big issue going into Haiti, and so the Department of Justice had a big play. More and more they came over and were working with the CINC, whereas in a normal situation, Justice would do justice, and never the twain would meet.

Student: Some of them, like the Department of State, which has an active role in any military operation ...

Oettinger: I should read you your Miranda rights. He's with the State Department.

Kelley: We do provide communications linkage for the State Department via some of our satellite capabilities and some of our networks. Others we help as needed, but aren't routinely in the network. But the State Department is absolutely critical, particularly for that CINC. It has to do all that negotiating with the in-country representative, so he has to have connections to all the ambassadors out there, plus back to the State Department in Washington.

Student: I don't want to belabor the point because I know you want to get on, but even within the State Department itself, when you take away task forces, there are a lot of stovepipe, organizational command and control and communications problems.

Kelley: We're not trying to solve that one. That's Fernando's problem.

Student: I wish you would, but I'm just interested in the context of the government as a whole having to come together in an interoperability arrangement to deal with more and more of these complicated efforts in pursuit of U.S. interests.

Kelley: One of the groups I've got in the engineering section works strictly on standards. They deal with the international arena. They're the representatives to all the NATO standards bodies. We've also tried to work within the government. In my other hat, I run the National Communications System, on which the Department of State has a representative. On that side of it, we try to work

on such issues as, for example, ATM or DMS to make sure that we as a government know what direction and what vector we're on so that opportunities for interoperability can be seized. They can't be directed, though. It's an interagency process. We're all collegial, and we go from there.

Student: On this interoperability question, a lot of people, especially NATO, try to downplay the problem of interoperability by saying it's really a doctrinal issue; it's not technological, it's not hardware. If you get to combined joint doctrine, you're going to be able to work together. What do you think of that argument?

Kelley: I think that's not a correct argument. I think it's all of the above. But it is technical also, and it goes back to industry. I understand this. Each nation wants full employment, everybody has to have a fair shot at the pie. That equity does not necessarily lend itself to interoperability, and that's just one example. But I do believe that it's an oversimplification to say that if we had common doctrine, then ergo we'd have a technical solution. That does not help. Look at the United States; we've proved that doesn't happen by chance, hardly ever. We still have internal interoperability problems. Many people will agree that this is what we're going to do to get to the right side of the chart (figure 19), but there is an infinite number of solutions on how to achieve that. That's why the standards are important, but they're not enough. I'll get into one of our command and control systems and how we're getting around that. But every time somebody will hook his hat on standards, and is that the answer? You can guarantee you're not going to have interoperability, because the standards aren't that good, especially with the emerging technology that we have right now.

Oettinger: I had a visitor from France this morning who was telling me a long story that I will not bore you with about the current ongoing argument between the European Union in Brussels, specifically Commissioner

Bangemann of DG XIII,⁵ and the chairman of the U.S. Federal Communications Commission over the standards for cellular telephones. The European view, as one would have expected, is that GSM⁶ should be the one standard; the U.S. view is there should be a plurality of standards that are not government dictated. This is going to go the way of the banana war. These two worlds intersect on those technological issues. They're "electro-political" issues.

Student: One more question on the technology issue, sir. You mentioned earlier the lieutenant, for example, who finds that nifty way of doing something. This is just in terms of technology. When you're trying to create those standards and address the interoperability, it seems like a direct trade-off with that creativity, that initiative. How can you still make creativity a viable option, as well as address the interoperability issues? It seems like a good criticism on switching that.

Kelley: It's a very fair criticism, and that's the argument. Today we're in a very fast-moving technological era. That's why I mentioned earlier that Ms. Dawn Hartley's job is to capture those new technologies to make sure they get inserted in what Pete is doing, because he's got a job to do to make sure that today's world is satisfied. I have another part of the organization that tries to look at tomorrow and see how quickly we can bring them together. But you can't ever become overenamored with standards and stability at the expense of hiding your head in the sand and missing a major technological wave that's going by.

If we had done a normal procurement on the way we're doing GCCS right now, we would not have any of the Web tools that are available to everybody in the military through the Internet. We'd still be writing up a request for proposals trying to specify it, instead of taking a different approach to the acquisition and getting right on with it so that

⁵ Martin Bangemann of Germany was the EU commissioner for information and telecommunications technologies.

⁶ The Groupe Spéciale Mobile (GSM) sets the European standards for mobile communications.

our tools are the most modern tools that exist today. But it's a constant balance you've always got to watch as you do this.

Oettinger: May I exploit this? You just said the magic words. I've been fanatical in the course about pointing out balancing acts, in this case balancing economic advantages versus a technical lock-in. If you don't standardize, you can't interoperate. It's a problem that doesn't get solved, precisely, as General Kelley has said, in a period of rapidly moving technology. In a period of relative stability, it may give the illusion that it can be solved, but in a rapidly moving period, it can't. So thinking about it in terms of balances is absolutely critical.

Paulson: Standards lag the technology by, in the best case, about two years, and in many cases more. There's a reason why the technology moves. It's because as a manufacturer you want to be unique. That is the way you sell your product. That is the way you capture market share. So it is not to your advantage to standardize in a rapidly changing technology. We are still trying to get security standards through the ATM forum that say, "These are the standards that we're going to apply in ATM." At the same time, we're also talking about the demise of ATM as a technology. It is going to go out of the marketplace and be replaced by another technology within what some people say is only another three or four years. So, if you look at standards as the means to enforce interoperability in this business, you will die. It helps, let me tell you, because when you get the two plugged together, it makes your gateways and your black-box interfaces a little bit easier to engineer and implement, but standards will not give you interoperability.

Student: Sir, I know that in business they very often do a rolling procurement, where when you have an outdated technology, it just drops down and someone who is a lot less mission critical can start using that technology, maybe in a training environment. But when you talk about this only in terms of interconnectivity—where you just mentioned that you have that new nifty technology that's making the ATM system obsolete—it seems

that everyone needs to be on board with that, and the rolling procurement can't necessarily take root. You'd lose so much infrastructure that you've already built.

Kelley: You've got to be careful. Let me give you a couple of examples. Voice-over IP is the new buzzword in technology; that and the gigabit ethernet.

Let's take voice-over IP. It's in the hype stage right now, and if you talk to my good friends over at Cisco, it's here today, a done deed, let's have it. Why are you so dumb that you can't see this? But what's not there? It gets back to the standards. There's no common way to set up calls on it from different manufacturers. That's why Cisco loves its system: stay inside Cisco and you've got the world beat. But is everybody on earth going to buy Cisco? No. So there has to be a multivendor standard, or at least some subset of the standard that they all agree to so that you can in fact have voice calls go globally, as we do now.

What are we going to do to replace Signaling System 7 in the voice-over IP world? We're getting into technical arguments here, but the bottom line is that your concerns are well placed and there's no simple answer. That's why there's the evolution that Pete's promoting. These labs work for him, too; he keeps a finger on them. The guy who runs the ATM lab reports to him, and Pete tells him what he wants him to do, and says, "I've got a problem here." What we're trying to do is bring together the today guy and the future guys and make them have a common vision of what needs to be done.

Oettinger: The hype is subtle. I have a voice link, and I could have a video-over IP link from my home to Chicago, because I have a new granddaughter there. It's \$99 for the equipment and software at one end, and \$99 for the equipment and software at the other end. You say, "Yes, what's the matter? It's not hype, it's real." However, every time I want to use it, in order to get things set up, I've in the first instance got to make a regular network phone call to my son to say, "Are you ready? Get it all hooked up," et cetera, because there is no way of finding him otherwise. I don't think you'd want to have your

military hooked up like that. The difference, then, between that hobby kind of setup and something that you'd want to rely on when you're being shot at is vast; it's huge.

Kelley: I think we've beaten this chart (figure 19) to death.

The only reason I put this slide up (figure 20) is to raise the issue of how you pay for this. How do you handle that, and how do you dampen appetites, because everybody wants everything if it's free? That's human nature, and we can attest to that. There are a lot of things in the command and control arena we did put out there that are considered free, so the requirements grow to be infinite.

AT&T and MCI are over on the left side, in the business area. When AT&T was around as a monopoly, they couldn't refuse service or unprofitable work because they were a benevolent monopoly. But now that we've broken it up, there is some argument that business can in fact say, "Heck, no. I just can't get a return on my investment. I'm not going to do it." I can't do that. So immediately I'm at a disadvantage when somebody says, "Well, I can get this from Sprint for X, and look what DISA is charging." But, oh, oh, I have to be able to bring back those guys

from Kosovo. Somehow I have to recover those kinds of charges for the global interconnectivity for that service. So it's an apples and oranges comparison.

The other side of it is that the services are sort of on the right. They mostly get appropriated dollars in this type of business, and to them, to the people using it, it appears free. That's a fact of life. At the high levels in the Army, Navy, or Air Force, they know they're paying the bills, but at the level at which it is being executed, it appears to be free.

Oettinger: This is familiar at Harvard as well. The students all have free e-mail and all forms of Internet access. The dean has noticed over the last year or two that his information technology bill has grown at 40 percent a year, and he's angry.

Kelley: We're very familiar with that exponential curve.

Paulson: We track it every day.

Kelley: We believe that as an agency we should be here in the middle, because we've obviously got to do some stuff for the

Business	Utility	Tax-Financed Provider
<p>For-profit motivation:</p> <ul style="list-style-type: none"> • Refusal of unprofitable work • Customer always equals person with funds <p>Enterprise equities not met:</p> <ul style="list-style-type: none"> • Global reach • Interoperability • Security • Surge capacity • Positive control 	<ul style="list-style-type: none"> • Finances and operations run for common good • Must support everyone • High visibility for costs and governed by public utility commission • Expected to provide some services below average cost • Commercial scheme (rates) regulates customer behavior • Guaranteed customer base and return 	<ul style="list-style-type: none"> • Service financed off top line of budgets, business cases rarely done • Services appear free to end users • Can shift cost to other users if utility also exists • Low/no visibility of costs vis-à-vis end product • Many costs are treated as sunk • Acquisition • Military personnel • Engineering • Facilities
<p><i>The enterprise requires a utility paradigm. Utilities can't behave entirely like businesses. More importantly, they will never compete successfully with a tax-financed provider.</i></p>		

Figure 20

Today's Funding and Mechanisms Undercut Joint and Enterprise Approach

common good. So, we think that "utility" best describes how we should approach our business. We don't want to give out the access that Pete's developed for free, because then we could never satisfy the requirements. There has to be some charge. But we do put things on there that the military needs—the surge capacity, the interoperability, the security. Those are things that AT&T and Sprint don't put on it. We have to make sure that all those things are added. We even use things from NSA for the encryption, for example, in our secure networks. All of that gets added into the pot for which we have to recover the costs. If we're not a utility now, we're suggesting that as a utility we would take that on as part of promoting the common good for everybody and then putting on usage charges for those people at a much reduced rate so they could compare to Sprint and say, "DISA's cheaper." Then we could enforce the behavior that we want for interoperability and security and being on the network and so forth. If you remember that pipe chart that Pete showed you (figure 10), we also make it so that everybody will move their networks to that very economic pipe by downsizing all the separate networks.

Now, here's how we show the cost of a T-1 service as \$6,100 per month (figure 21). This is a notional example. The Army, Navy, and Air Force talk to Sprint, and Sprint says they can get it for \$3,000 to \$3,600. But, guess what! That's the way they see it, but here are all the other things that have to be paid for to make the right side equivalent to the left, and guess what the cost is to the department—the same or more over in the private sector. It's the tip of the iceberg theory. Again, we understand that we've inspired people to act based on this, and that's a rational act from their perspective, but not from DOD's standpoint. So we need to change that mindset. That's why we're looking at the utility paradigm.

This is the dynamic (figure 22). Everybody knows that some people's phone rates are going down. The rates in this business are going down; there's no question about it. But unfortunately, we're seeing the same demand curve that the dean is seeing, only it's more than 40 percent.

Paulson: We're seeing about 100 percent on the data side, but probably only 4 to 8 percent on the voice side. The data demand is just going crazy.

Kelley: This then completely wipes out the decreasing trend in the rates, which is a very helpful trend for the prices. The unit costs go down, but your aggregate, total cost, is going up for everybody. This goes back to your VTC concern, because most of the applications we're looking at today are broadband—imagery, VTC. Those kinds of things are going to drive the cost up just by virtue of the demands they put on it.

Very quickly I'll give you a couple of shots on the other pillar programs. We've discussed one in detail: the one that Pete's running.

We've talked a little about GCCS (figure 23). Remember, what we mentioned was the vision that came out of Desert Storm: a fused, real-time, true picture of the battlespace. This is the implementation of a system that for the first time in history uses modern technology. This is an intranet. We use all the Web technologies on it, but it's separate from any other network because it's at the Secret level, and we have the encryption that segregates it off. That gives it tremendous power for these CINCs to exchange information. We're looking at Y2K compliance. We're at the point now where we're just working on the interfaces. Everything else has been done and tested. We've got the majority of the interfaces done now; these are interfaces with systems I don't control, but need to pull information from. So in fact we're closing that out right now.

A lot of this is based on Sun Solaris and Hewlett-Packard equipment, but we're in the process of bringing it down to the NT box from a cost standpoint and from a training standpoint. It's far easier to bring people up to speed in NT as opposed to UNIX.

Oettinger: Before you go on, for the sake of continuity, in previous years of the seminar, and these folks may want to do some reading, we've heard a lot about WWMCCS, the Worldwide Military Command and Control System. What is the relationship? Is it completely separate? Is it an outgrowth?

	DISA's view (DWCF)	MilDeps view (appropriated)
Apparent customer costs	<div>\$6,100/month</div> <div>Service</div> <div>Data service (T-1 speed)</div>	<div>\$3,100-\$3,600/month</div> <div>Transmission</div> <div>T-1 transmission circuit</div>
Hidden costs	None	<div>Operations</div> <ul style="list-style-type: none"> • Interoperability • Backbone operations cost (O&M, depreciation) <ul style="list-style-type: none"> – Bandwidth management – Data switching • Provisioning • Billing • Military features • Network management • Router operations costs <div>\$3,000-\$4,000/month</div>
Cost to DOD	\$6,100/month	\$6,100-\$7,600/month

DWCF = Defense Working Capital Fund

Figure 21

Implications of the Two Views: Data Service Example

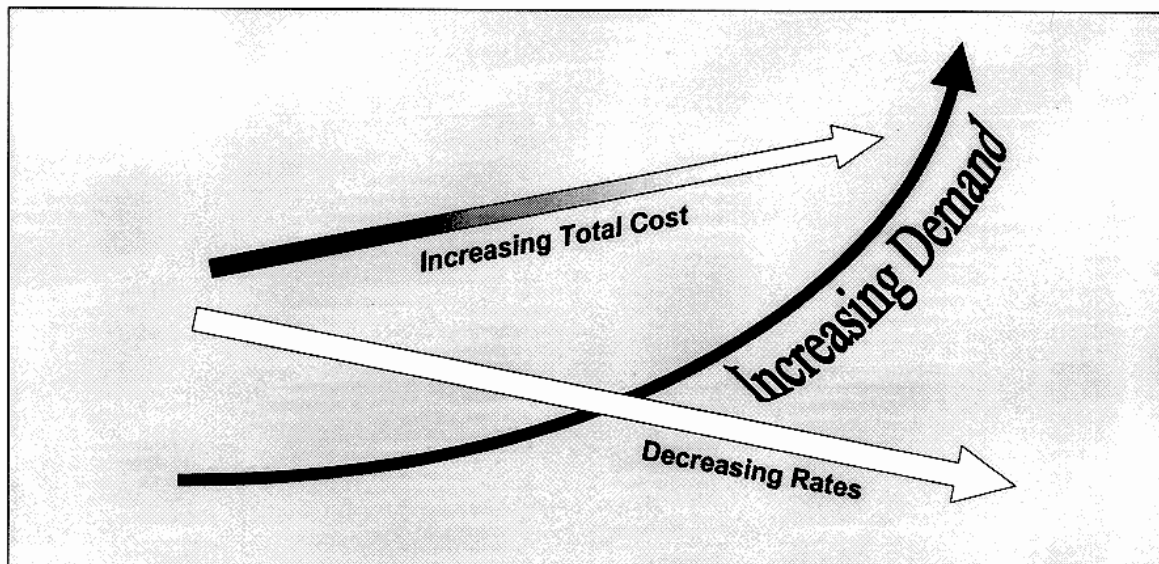


Figure 22

DOD's Telecom Challenge

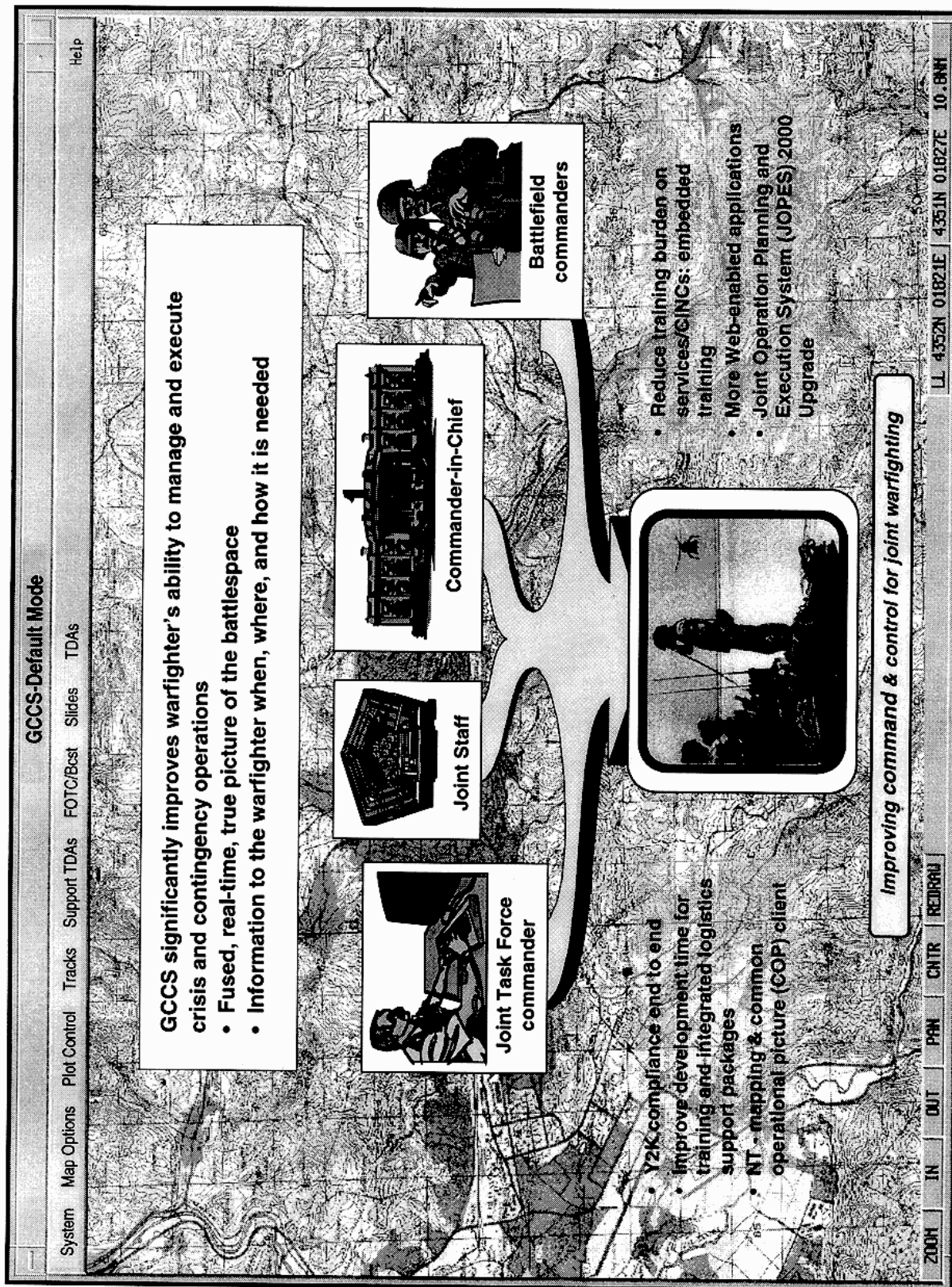


Figure 23
Global Command & Control System (GCCS): The Way Ahead

Kelley: The relation is: anything you know about WWMCCS, you may flush, because we have killed it. In fact, I was at the dedication where they turned over one of the terminals to the Smithsonian.

Oettinger: So that's history?

Kelley: It is history. This system replaced it. We did it, again, in that two-year warp speed for DOD-type acquisition. My predecessor started this, and this system is constantly evolving. Again, the job of Dawn Hartley and my advanced technology folks is to look at this and make sure we're inserting all the new technologies that would be of value to a warfighter.

This is an example (figure 24). This is Special Operations Command and Southern Command, which focuses largely on South America. The two also worked together on a drug operation and they exchanged a common picture between their terminals. Now, that sounds trivial, but that was something that couldn't be done with WWMCCS, and it was very useful.

***Adapting the GCCS COP in support of
USSOCOM and USSOUTHCOM***

SOC SOUTH SEALs rescued survivors early in the relief effort using Zodiac boats to reach flooded areas not accessible by vehicle. USSOCOM requested that SOC SOUTH provide position information on the deployed special operations force using the GCCS common operational picture (COP). The GCCS noncommissioned officer in charge, SFC Bruce Smith, with assistance from DISA CENTCOM/SOCOM technical experts Dick Clark and Marie Roberts, created the link for GCCS COP information transfer between USSOUTHCOM and USSOCOM.

Figure 24

Supporting the Warfighter: Hurricane Mitch

Here is the GCCS that I've been talking about (figure 25), where I want to take all of these common applications, drive them to GCCS, run them on common hardware and

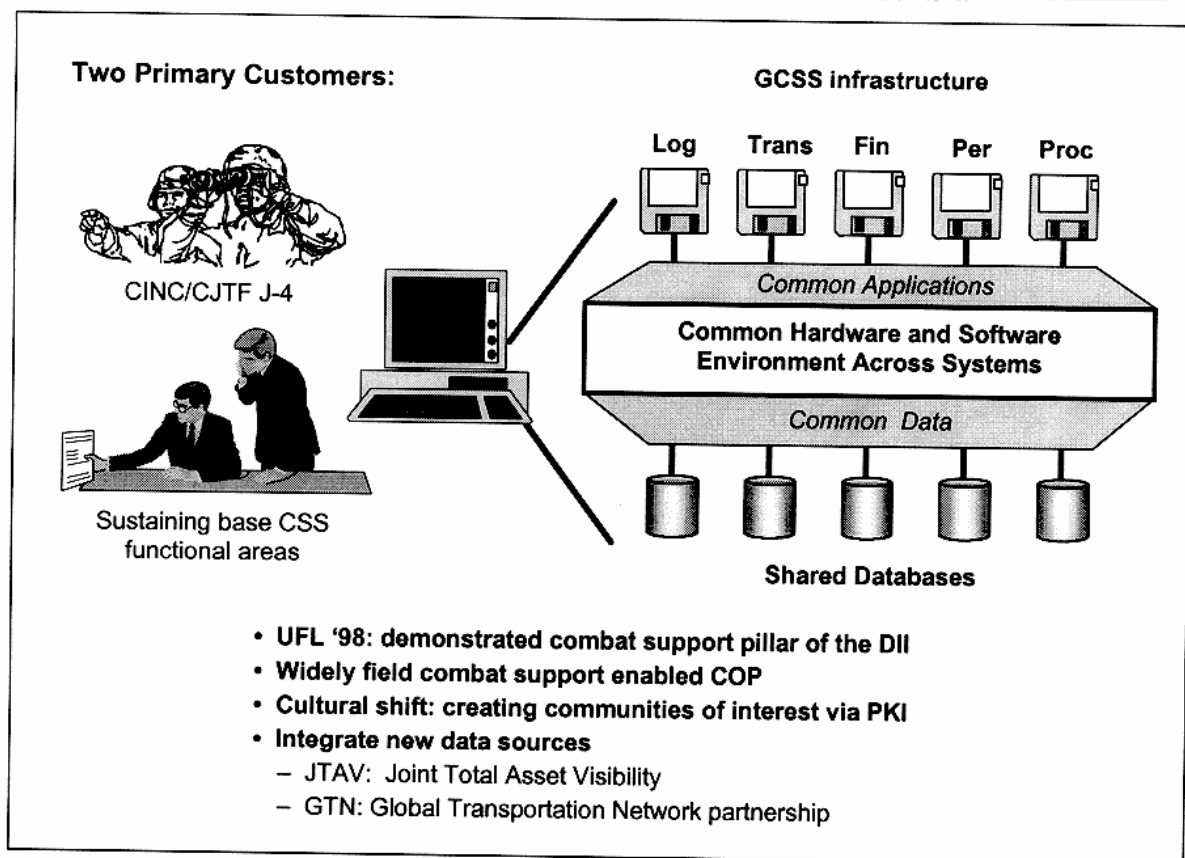
software, get to the data that you need, and then be able to show them on the same terminal. You get a GCCS picture of the battlespace that lets you surround that battlespace picture with information on the logistics aspect, or medical aspect; whatever you happen to need at the time. You can then relate what's going on in the tactical battlefield to your logistics capability to support it. That's what we demonstrated in Korea very recently.

The J-4 on the Joint Staff is the functional requirements guy on this system, and we work very closely with him and with the Deputy CINC at TRANSCOM, because that's where we get all our visibility. One of the other lessons from Desert Storm was in-transit visibility. We couldn't keep track of things that were coming over, and when they did get there, we didn't know where they were.⁷ Things just started piling up on the wharves. This system now will let us attack that problem with in-transit visibility all the way over, so we know what's coming. That, obviously, has implications for strategic lift: we'll be able to reduce what we have to send because we'll know what we've got.

What we're trying to do here with our DMS development is to get a real merger between our equipment and what's going on in the commercial world (figure 26). Right now I can use the DMS on my portable computer. It looks like Microsoft Outlook to me, except it's got two additional buttons on it with which I can encrypt the message. I can digitally sign the message, and then I can send it back to my office and give them something sensitive that could go any way, through the Internet or whatever; it doesn't matter. That is a tremendously powerful tool.

But we want to try to keep this convergence going. Right now I'm on Microsoft Outlook. Lotus also has a client that works in the DMS world. We thought that the business-grade messaging would come along faster because of different things driving it in the industry, and it just has not. So, we're still watching it closely, but we're not

⁷ See Robert Lawrence, "Global Reach Laydown," in seminar proceedings, 1995, for a detailed description of this problem; see also Richard T. Reynolds, "The Pitfalls of Peacetime Military Bureaucracy," in seminar proceedings, 1996.



UFL = Ulchi Focus Lens (military exercise)

Figure 25
GCSS: The Way Ahead

sanguine that it's going to converge as soon as we would have wanted it to.

Student: In one part of the State Department's five-to-seven-year plan for communications, there is a vision that the typical, traditional State Department telegram is going to die and we will no longer have Embassy Cable 123 from Bonn or whatever. I was up in Ottawa earlier this week and met with people in their foreign ministry, and in effect the Canadian foreign affairs establishment no longer has a cable system. They've gone to a huge intranet around the world with the whole Canadian government. But the military in Canada is excluded from that. The military is maintaining their own system. I was wondering if there were any thought or any trend within the U.S. military to do away with the traditional messaging and archiving system as we know it today.

Kelley: Do you mean the AUTODIN (Automatic Digital Network) messaging?

Student: I mean just the numbering and the format in the standard kind of message.

Kelley: I'm not a big fan of those formatted messages. In my military career, I can't ever remember getting one that I really acted on. It could be that people were just leaving me out of the loop.

We are, in fact, closing down our AUTODIN system. De facto it's being closed for us. E-mail has sort of taken on the load. We've seen a tremendous drop in the number of messages we send through the formal messaging system, and for many good reasons. With e-mail, I can send it out and, bang! I get an immediate response. It doesn't have to go through all those manual steps.

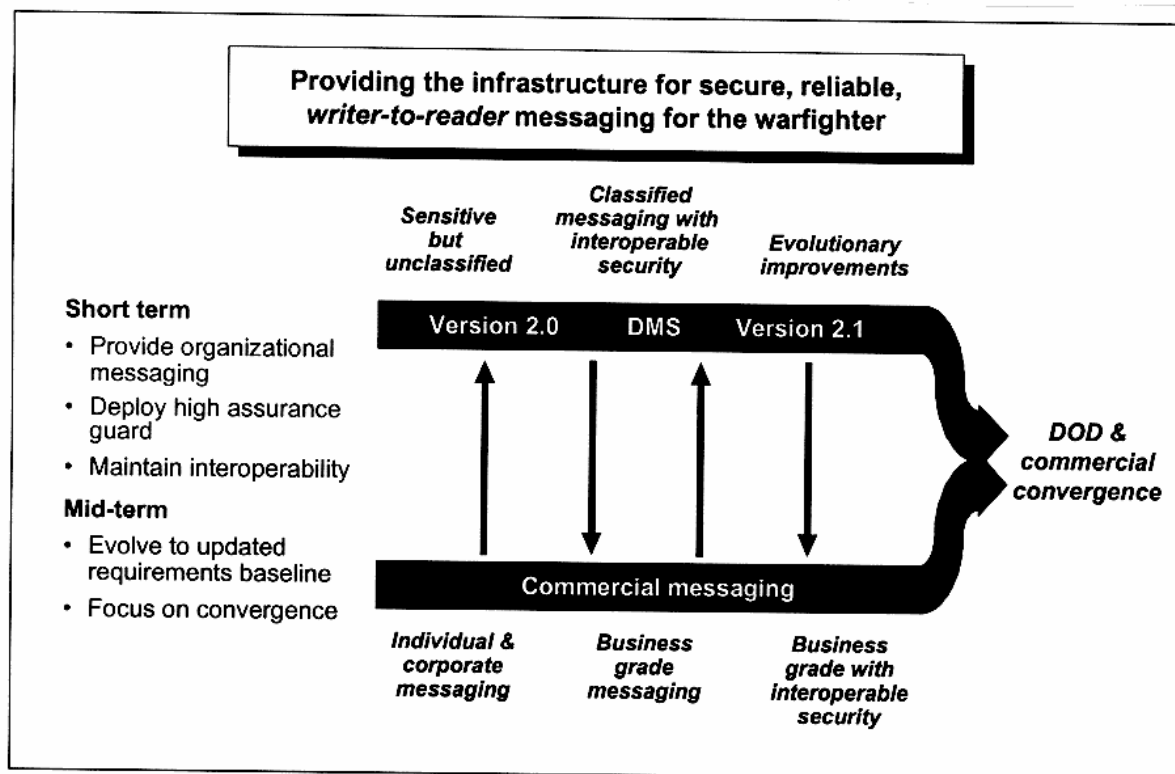


Figure 26
Defense Message System (DMS): the Way Ahead

We've taken out the middleman with e-mail. We want to do the same thing with DMS.

Student: How do you deal with archiving and retrieval?

Kelley: That's for the historians to worry about! Actually, that is a tough question, and I don't have a good answer for it. Ever since I observed what happened to Ollie North and a few other people with e-mail, I personally am very careful about what I write in e-mail. But the archiving and how we're going to handle it is being sorted out in DOD right now. We do have a working group on records management that's going on. My chief information officer is involved in it.

Information assurance is a new growth topic (figure 27). Here's the Defense Department. Notice the national structure, the global structure. This is an issue with no boundaries at all. You have to recognize that we used to like to think of ourselves as a closed system that suffers little effect from

what goes on around us. That's not true in this business of information assurance.

Here are some of the problems. We've already talked about standards in the comm world and in the information world (figure 28). In the information assurance world, there are zip standards right now because it has moved so fast. The big "A" and the little "a" have to do with whether the attack comes from hackers who are just trying to see if they can exploit your system, or if it's some coordinated state-sponsored attack that could in fact do harm to the nation. That's not easy to decide when you first start getting symptoms of the attacks. I've already mentioned the lack of borders.

Regarding complexity, these networks are like living organisms. They're not simplistic line diagrams on a chart. Do you remember Pete's chart of what DISN looked like before we redid the United States (figure 13)? There are still many networks globally that look like that, so it's very difficult to define the battlespace, to know what the

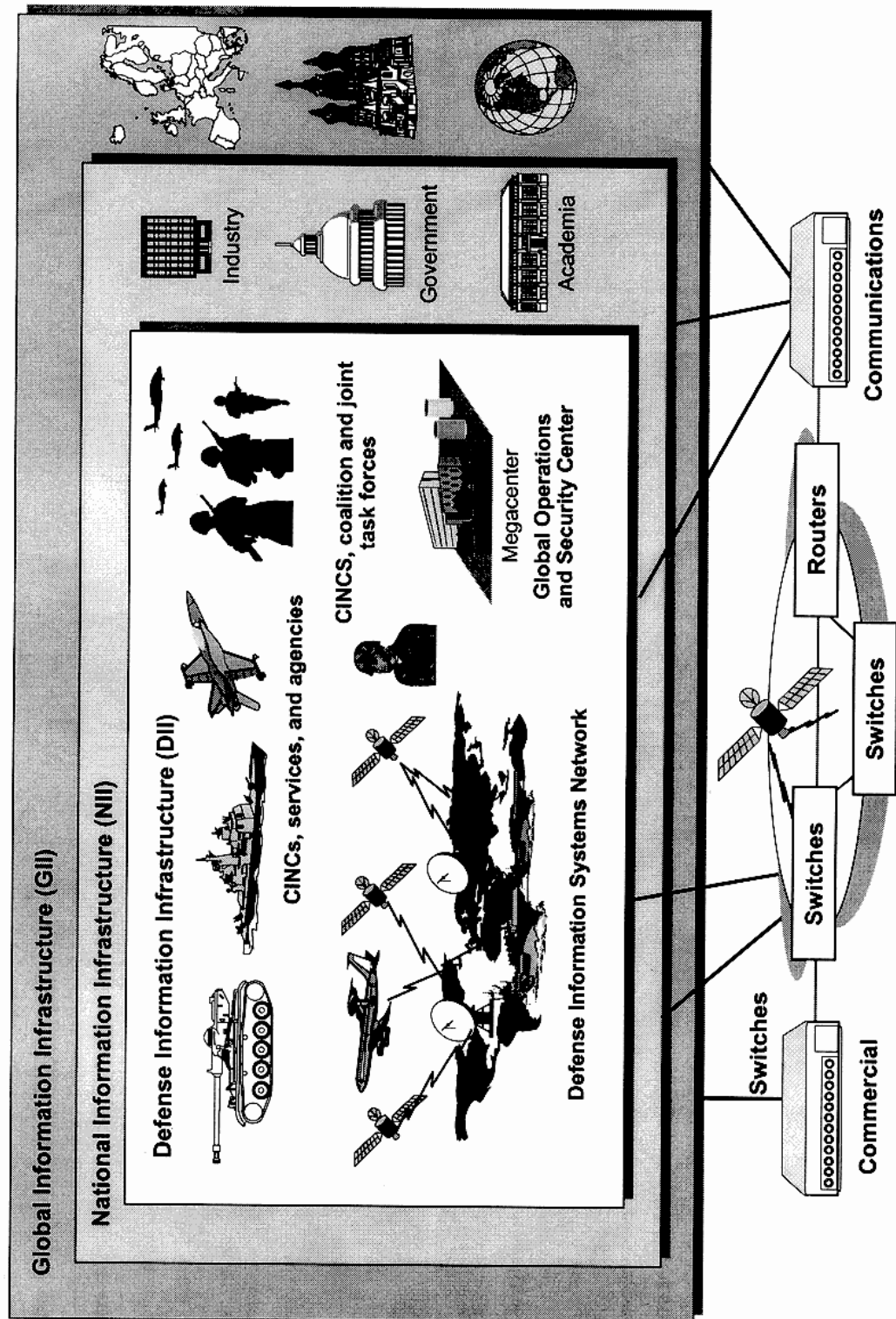


Figure 27
 Harnessing the Power of the Network for the Warfighter

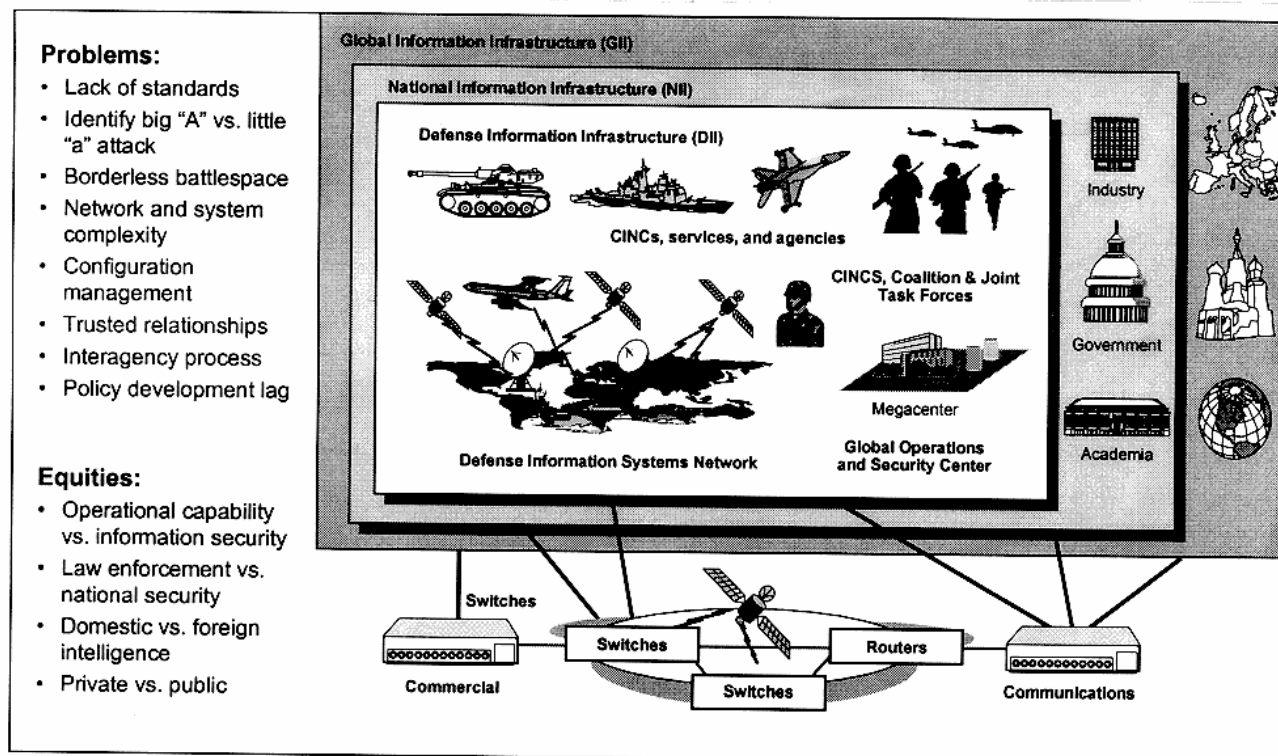


Figure 28
Information Assurance: The Big Picture

friendly territory is and what the enemy territory is.

When we get into the equities, we work very closely with the Department of Justice. But the equity that the military has is not always the same equity the Justice Department has. Their job is to find, prosecute, and convict criminals and people who break the law. Our job is not necessarily to go after law-breakers, but we don't want them interfering with a system, and thereby maybe interfering with our operations. So we may want to take a kinetic solution as opposed to a legal solution. (That's a euphemism for "We may want to shoot them.") Because, in the military, if we have an ongoing operation and somebody is really tearing up our command and control network, one of the first things we do is go after the bad guys' command and control network. We just did that in Kosovo, and so it's logical to assume that people will come after ours. What we're saying is we don't want to limit ourselves to a response in kind if somebody does that.

Student: Sir, from a civilian standpoint that seems kind of scary, in case your kinetic solution, or your hack-back solution, had repercussions or cascading failures on the system as a whole, which creates a whole new legal liability for the Defense Department. Right now we don't have a CONUS CINC or anything like that, domestic antiterrorism ...

Kelley: We're going to have one of those, so stand by.

Student: I just wanted to get any thoughts on that solution.

Kelley: You've hit on a real problem. The kinetic solution I was talking about was not hacking back, it was a bomb. But hacking back does bring up every issue that you just mentioned. We've been through many of these attacks now, and eventually, in almost every case, we've identified the perpetrator, but not necessarily the right one the first time. On a hack-back, we'd want to go back im-

mediately to try to stop them, especially if we're in an operation and they were causing some sort of interruption. The details of how we're going to work all that out have not been decided. The law has a long way to go in this also.

Oettinger: By way of a footnote for those who are interested in the Justice Department side of this whole question, there is a talk from 1997 by Phil Heymann, the former deputy attorney general of the criminal justice division, looking at it from the point of view of the prosecutor, and it's a very different view.⁸ What they're looking for and how they want to react is very different. It's a significant political problem to reconcile these things, and the process is ongoing. It's far from being anywhere near a stable resolution.

Kelley: Right, but I wouldn't want to give you the impression that we're in one camp, and the law guys are in the other. That's not true. I have legal guys who are working with my JTF in the building, and we also have Defense Department employees working in the National Infrastructure Protection Center, so we're working together. In fact, I've had more meetings with Janet Reno than I care to count on this subject. I've never seen so many lawyers, but they're all very smart, very dedicated Americans, and we're all trying to grope our way through the problem that you raised. What are the legal issues, and how do we ensure security? There are technical issues also, and there's the idea of first making sure that the entity you target to hack back is the right target.

Student: I have one more question, sir. Was any component there in Eligible Receiver?⁹

⁸ Philip B. Heymann, "Relationships Between Law Enforcement and Intelligence in the Post-Cold War Era," in seminar proceedings, spring 1997.

⁹ Eligible Receiver was a Pentagon exercise conducted in 1997, in which NSA employees used commercial off-the-shelf technology and software from hacker Web sites to penetrate unclassified DOD computer systems.

Kelley: There were no hack-backs in Eligible Receiver.

In so many things we do in this business, technology may be the major part of a problem, but it's certainly not the only part of an answer (figure 29). I'll be very candid with you. In the last two or three years, I've had four heads of my global CERT (computer emergency response team). I can't keep them because of the demand and the salaries that are being paid on the outside right now in this business. You don't hear about it in the press, but people in the banking industry are worried. They're hiring everybody they can to get their stuff squared away, because the financial center is very open in the United States. People are really trying to close those doors. Keeping good people is difficult.

I don't know if you talked about the policy side, Presidential Decision Directive 63 (PDD 63).

Oettinger: Yes, they're aware of it. Some may even have read the unclassified version because it's available on the Internet.

Kelley: Yes, it's a national problem. This is not just a Defense Department problem. It's a whole new way the United States needs to think about defending itself. It used to be we worried about borders, and they were pretty well defined. We could look at the issue and say, "This is what we do, and this you shall not cross under penalty of we're going to zap you." You can't say that in cyberspace, and you can't say it for our water system, our power grid, our FAA, our financial system, you name it. They all have links into this business that we're talking about for control and so forth. So, this PDD is calling for a whole new thought process.

In the Department of Defense, we've come to the realization that there is no silver bullet in this business, so we're going to develop a defense-in-depth strategy. We have a series of places where we try to put up barriers, and we keep raising the bar. Depending on the value of the information, the bar is so damn high that nobody's been able to hack it. There are other cases where we're just learning that we've got other vulnerabilities, particularly in the unclassified information. It's now so easy to aggregate it with a Web

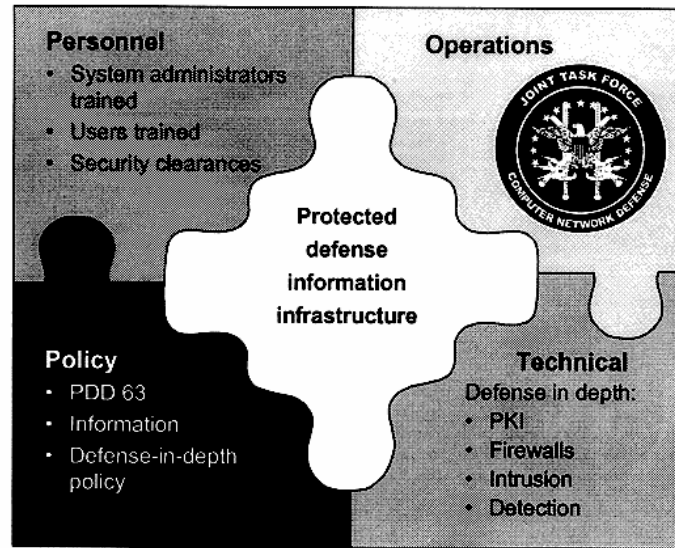


Figure 29
Information Assurance

search engine that it does create a vulnerability that never existed before. If you can aggregate enough unclassified information, you can figure out what the next operation may be by looking at the logistics flow and the personnel flow and all the rest of it.

Our strategy says, "Hey, we'd better re-think how we're handling this." That's why you've seen in the press a lot of things about the Web sites. I have a whole new organization that's being formed that works in my reserve component that will do Web site red teaming to make sure that we're not putting out information over the Web sites that we shouldn't. That's the operations piece I'll talk about: it is in fact the JTF.

I've discussed personnel, I think (figure 30).

Oettinger: Could I just bring you back for a moment to the reserve red teams on the sites that you have? They were created because of the difficulties of communicating among one's own group. Now, if you push that too far, you'll end up obviously securing everything, but we'll be back up the other pole of nobody being able to find out what they're supposed to find out. Then you have a Desert One sort of thing, where OPSEC was so important that the folks didn't know what the

others were doing. Could you say a few words about how you envision striking a balance in that?

Kelley: I was going to say that it sounds like another one of your balance examples.

Oettinger: It's exactly what I'm asking you. How would you strike it?

Kelley: I'll tell you what I'm doing in my agency, and I'm using myself as a prototype. Are you familiar with public key infrastructures (PKIs) and that kind of technology?

- **Formal system administrator training and certification**
 - Multiple levels
 - Operating system specific
 - Written test at all levels and operations test at higher levels
- **User computer security training**
- **Security clearances**

Figure 30
Personnel

I've put my Web sites behind a PKI at DISA. We've issued over 5,000 certificates to my employees and to some of my contractors so that they can get the information that they need. But, by the same token, I've now eliminated a large part of the world that previously could have just hacked into the site. So, the PKI is one tool in our defense-in-depth strategy. We have more than 6,000 people with certificates now who can get on it, and you can also use it for digital signature purposes. That's just the beginning.

We don't have the scalable solution. That's the other thing I would tell you. Any time we found a solution in the security area, the Achilles heel of it has been that we say, "Okay, it works great for these 50 or 100 things." If we try to scale it to 10,000 or to 2 million, guess what? It doesn't work. Scalability is not a given. It has to be engineered in the beginning.

The other thing I'll tell you is that we developed prototypes in this and other areas and our customers are so pressured to get into doing things in the paperless way, and to save money, and to reduce staff, that they take a prototype and, unbeknownst to us, it becomes the operational system. Then we start getting phone calls saying, "Hey, what the hell?" Well, what we thought was a prototype with 100 people has 3,000 on it, and it's going to 10,000. So this whole business of scalability is another issue involved here, just like balance.

Student: Sir, since you mentioned PKI, it seems great for authentication and, I guess, general security, but unnecessary for the integrity of the system. You don't necessarily need that certificate to come in and maybe plant some of those insidious kind of viruses.

Kelley: That's a good point, and a lot of folks at Defense don't understand that. Because of the hype that has surrounded PKI, they think it's a silver bullet, and they think that because you implement a PKI, everything is okay. Not true, for exactly the reason you just mentioned: you can implant viruses. There are still many other ways you can do that. It may be useful to restrict viewing of a certain amount of data, but it doesn't say anything about service-denial attacks. So

that's why there's the defense-in-depth strategy. But, boy, I'll tell you, we're still fighting it in the Defense Department right now: getting people to understand that, so we don't put out a very restrictive little policy and later people say, "Why in hell did they do that?" It doesn't work. We're trying to avoid doing that.

Student: Do you think that is going to help you with your general access, your home pages, or your Web sites? What is the answer, beyond moving the information that was up on the Web into a classified state in some kind of effort to avoid aggregation? Is there any other way of defending against the aggregation?

Kelley: Access control is the big thing that you try to do to stop that so you don't have these search engines going against your Web sites and all that sort of stuff. Again, there is no simple answer. I think it's a host of actions that you can take, like restricting certain information. In the old days we never even considered a lot of the information to be of great value because it was so diffuse and it was very difficult to glean any intelligence out of it. Now, we're going to have to go through and do the information assessment phase to decide what has value. The PKI is a tool and a technique, but it is not the only and final answer. It can, in fact, protect your Web pages; you can control access with PKI. But then, guess what you take on? It's the whole other burden of administering the PKI, because it's only as good as the policy behind it. So to whom do you give a certificate? If you give them to everybody, what have you got? You've got an open door again. There's no free lunch, and we're back to the balancing act.

The JTF is the first of its kind (figure 31). It is not the end-all answer. The whole thrust behind the JTF was to get it started. We'll learn as we go. We will expand. It's a very small organization. But over time, we will see what we have to do to make it better. It is primarily focused on information assurance, not information operations. There's a subtle difference here. These guys are not tasked to go out and charge into Iraq and take down a system. That's not their mission.

- Joint Task Force: Computer Network Defense (JTF-CND)
- First organization of its kind
- First step in defining how DOD will defend against this new threat
- Vice director of DISA dual-hatted as commander of the JTF
- Initial operational capability: 30 December 1998
- Full operational capability: June 1999 (projected)

Figure 31
Operations

Subject to the authority and direction of the SECDEF, JTF-CND will, in conjunction with the unified commands, services, and agencies, be responsible for coordinating and directing the defense of DOD computer systems and computer networks. This mission includes the coordination of DOD defensive actions with non-DOD government agencies and appropriate private organizations.

JTF Charter,
4 December 1998

Figure 33
Mission

They're not the offensive guys. They're defensive.

Now, should offense and defense be together? That's a debate that's going on. A lot of people believe yes, and I think over time it will probably evolve that way, but right now, they're not. My vice director is the head honcho. It started this past December. June, which is not far off, is when we project that the JTF will be up and fully running.

This chart tries to answer all the press issues (figure 32). We've been slammed in the press: chain of command and blah, blah, blah. So, we just try to say to them, "Yes, we're aware that this is an interim step. It's not the final solution."

- It is an interim solution pending unified command process
- It is consistent with joint doctrine
- It provides *authorities* for unified action.
- It provides operational chain of command

*Answers the question,
"Who's in charge?"*

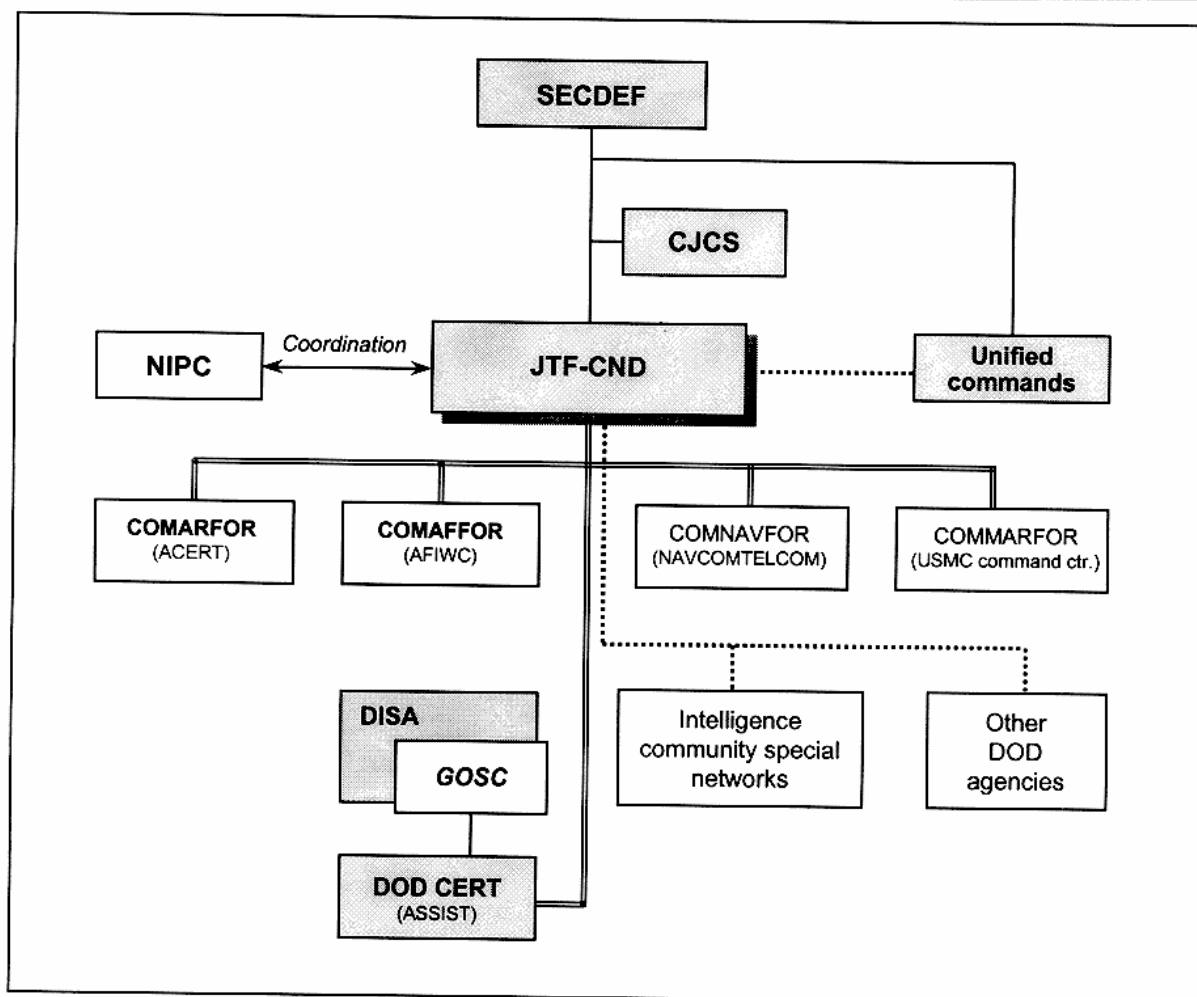
Figure 32
Why a Joint Task Force?

This is the JTF mission (figure 33). They will work largely for the CINCs, for the unified commands, to make sure that they're protected.

This is the chain of command (figure 34). I think that very shortly SPACECOM will be in here as the CINC to whom the JTF reports. They have components from all the services. My DISA organization includes the Global Operations Security Center. What we have done in DISA is merge network management and security absolutely. All the people are integrated. They're one organization, with the same boss, and that has really moved us light years forward. When you heard about the security guys sitting off on one side in the back room, not much was happening on the networks. Now that we've brought them together, we've got the synergy, and a lot has happened to make our networks one hell of a lot better and a lot harder. We do have very close links with intel, with NSA, and so forth, so they can bring their expertise to bear when we perceive ourselves to be under attack or strike.

I think we've already talked about PDD 63 (figure 35).

I talked a little bit about defense in depth, and in this concept we get out to the network level, where Pete operates (figure 36). We want to make sure those networks are available. Service-denial attacks are what really concern us at this level. Then the question is how we protect logical enclaves, and this sort of gets to your question of how we protect against aggregation of data. A firewall-type policy can be set up here to restrict who is allowed into the enclave; there's IP filtering, and there is a host of techniques that you can use.



ACERT = Army Computer Emergency Response Team
 AFIWC = Air Force Information Warfare Center
 ASSIST = Automated Systems Security Incident Support Team
 — = TACON
 = Coordinating authority

Figure 34
Command Relationships

Where we have found most of our vulnerabilities is in a lack of training of the person who is responsible for the system, the systems administrator. Why is that? You know I have trouble keeping the head of the organization. I have trouble keeping systems administrators right now! There is a massive churn in this business in the Washington, D.C., area. The one overriding principle is that there are no silver bullets.

Student: Just a quick question on that. Are most of your system administrators grown within the department itself, like enlisted personnel?

Kelley: It's a mixture. It's enlisted and civilian, both.

We've talked about defense in depth, and I've alluded to some of these things that we're looking at (figure 37). We really have been putting some effort into the processes to make sure that when we let somebody on the network they've done the right things; that they're not bringing a host of vulnerabilities behind them. So we have a very rigorous process for connection to the classified networks. In fact, we're also looking at how we do this in the unclassified world. The answer is, "Very carefully," because it's a hell of a lot bigger.

- "...protect nation's critical infrastructures from intentional attacks
- Public-private partnership (federal government lead agencies and private sector liaison officials)
- National Infrastructure Protection Center (NIPC)
 - Coordinates federal threat investigation, attack mitigation and response
 - FBI lead with representatives from DOD, Secret Service, Energy, Transportation, Intelligence, private sector
 - Projected 125 full-time employees

Note: for full text: <http://www.info-sec.com/ciao>

Figure 35

Policy: Presidential Decision Directive 63

The objective is to protect the networks, and then if we fail in that, to detect that something has gone wrong by putting up these barriers. Again, this goes back to the comment, "I've got people looking at technology to define the steady state of the network." The amount of information that flows over it is massive, but there are processes and mathematical models that can sort of say, "The parameters of this network typically operate in *this* band." If we see something out of band—and typical attacks have a signature that shows up—we want automated systems to be able to detect that so that the network itself can tell us when it's under attack. Right now that doesn't really happen. We have to analyze what's going on by looking at logs and that sort of thing. I predict that we'll have tools in the next two years. We're working very closely with Carnegie Mellon University, one of our CERTs, and we also have

- Defense in depth—the key
- Must work in conjunction with personnel, operations, and policy
- Cost and interoperability are major challenges

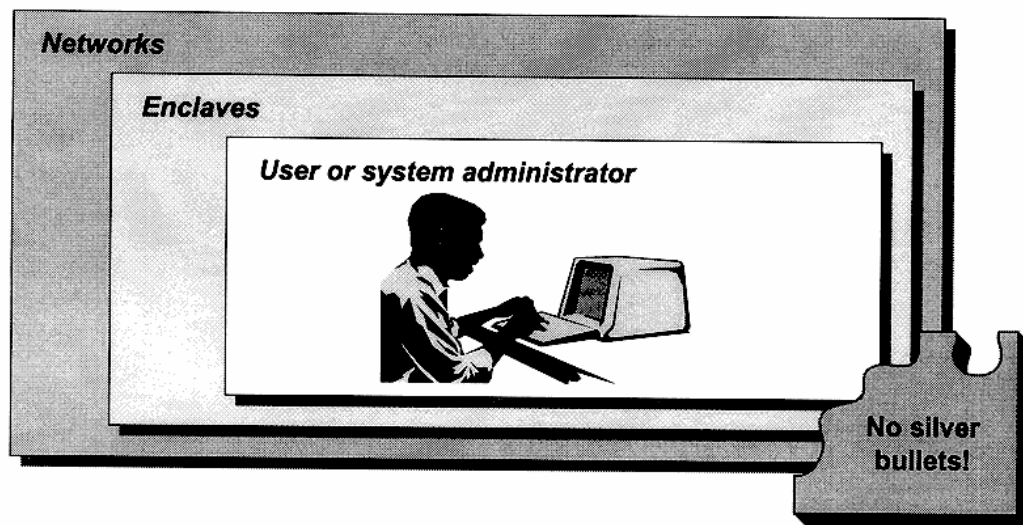


Figure 36

Technical

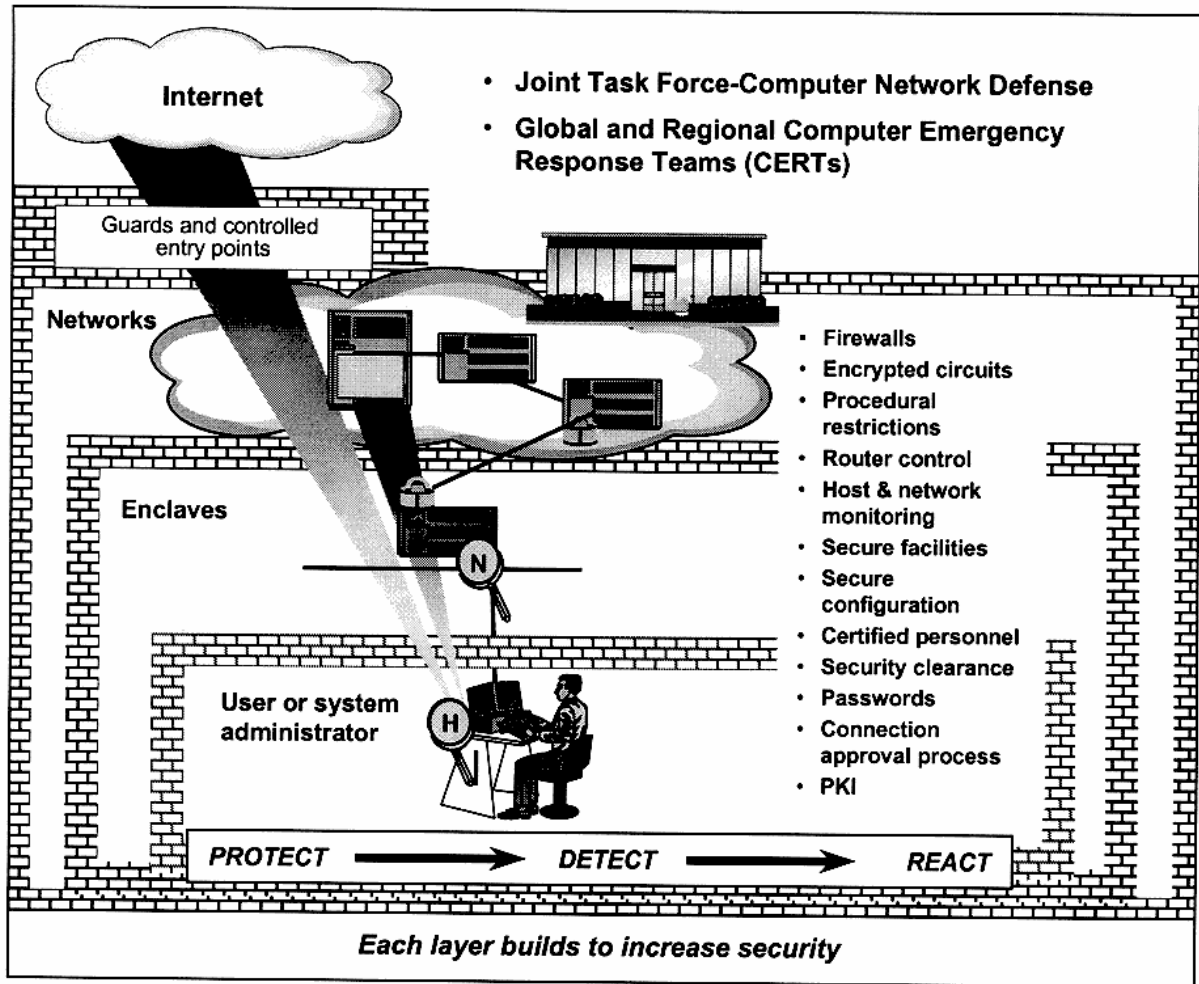


Figure 37
Defense in Depth

several contractors working on those kinds of tools.

We've talked about interoperability (figure 38). This is the heartstring chart I use. We have discussed this, but I'll tell you: de facto interoperability is important, but it's so important that unfortunately we put it on the JTF commander and the coalition forces and components during battle or peacekeeping operations. They're the ones who really work out the issues that these guys on the right (and notice that I've put myself with them) can't work out.

What's the dynamic there? I'll tell you. It's human nature, and it's compromise, and what I call the Beltway Syndrome. Meetings in the Pentagon can be very vicious in a time of declining resources. So the action officers

go in there, and they all know there's a critical component each service needs—be it a tank, a new aircraft, whatever—that they are not being funded for. So they're looking for every dime they can get to make sure that their core competencies—to train, equip, and be ready to fight—are in fact supported. It's not that they're bad Americans; they just know their shortfalls. Then we come in and start arguing about, "Hey, we've got to take a bigger view of what's going on in the 21st century, of this new type of warfare, and this network that gives us so much power brings us the vulnerability." It's a hard, hard sell in the building. So, what happens? Typically (it's human nature), there will be a compromise. If you can't agree with somebody at the table, you'll make a compromise. You don't

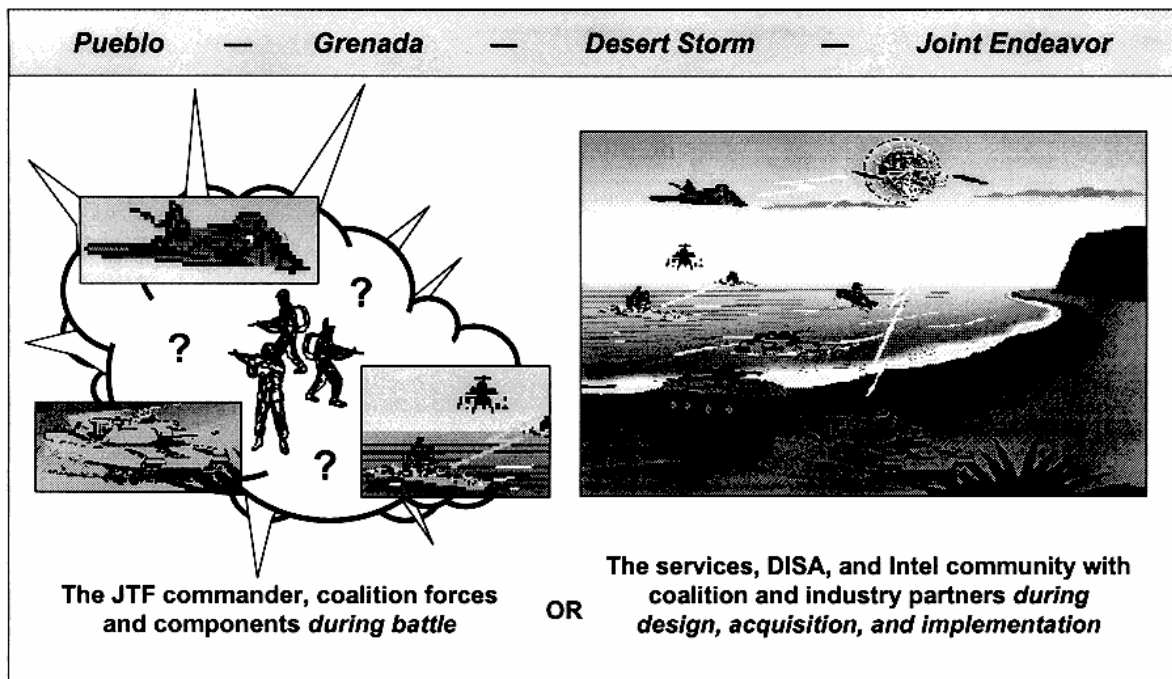


Figure 38

Who Should Work DOD Interoperability/Integration Issues?

get what you want; they don't get what they want, but the bottom line is that sometimes those Pentagon and Beltway compromises over on the right are not effective in warfare. People die. So this commander on the left of the slide says, "Uh, uh. I don't know who made the compromise back in Washington, but it doesn't work in the field." That goes back to all those functions again.

Oettinger: You may be wearing too much of a hairshirt for the Pentagon. Let me try out a point, going back to the NATO point and the responsibility beyond the military. The general used the words "procure, equip ..."

Kelley: "...train, maintain." These are the Title 10 terms.

Oettinger: These are not sort of magic words pulled out of the Pentagon hat. They are the words of the law. Title 10 of the National Security Act of 1947 put those responsibilities squarely on the military services. You might ask, "Why do such things remain?" There are many reasons, but one of them is that the Congress of the United

States, in its wisdom, wishes us to remain that way because the services and their procurement activities are like post offices and so on: spread across congressional districts. Even if the military were willing, within the Pentagon, to compromise to a certain extent, they've got to look over their shoulders at Title 10 and they've got to obey Title 10. The minute you touch these things here, which look like compromises, the waves you make go far beyond the Pentagon. This is fundamental bread-and-butter politics. The details are specific to the United States, but, as indicated earlier in mentioning NATO, the motivations and the dynamics are very similar in any country, in any alliance. If you look at it without understanding that, then you don't get a good grasp of what's really going on, which is why I wanted to make sure they understood that this is beyond your modest statement of its being intra-Pentagon. The responsibility goes back much further than that.

Kelley: I'm trying to be politically correct. I have served in NATO, but I'm restricting my comments to the United States.

We talked about some of these issues (figure 39). Industry and market share probably is the number one roadblock, and that's across all nations. I've had meetings with the highest levels of American industry—John Chambers, CEO of CISCO, Inc.; Jim Barksdale, former president and CEO of Netscape, Inc.; Scott McNealy, the CEO of Sun—and every one of them is a great

- **Industry—market share**
- **CINCs/services/agencies**
 - Not invented here
 - Need for control
 - Managed by different appropriation
- **Reduced spectrum**
- **Technology turnover**

Figure 39
Roadblocks to interoperability

American. But all of them have a corporate responsibility to their stockholders, so that's what they're interested in. They'll let me talk about interoperability, and they will listen, and then they will do what they can within their sphere as long as it doesn't affect their proprietary niche in the market. So we just have to be smart enough to understand that and figure out how we write contracts that bring them over the line to where we want them to be. That's something that sounds easy, but it's not often done in practice because we change over a lot.

Oettinger: Let me interject a point back to Kawika Daguio's presentation.¹⁰ At least he's got contracts to give, which give some incentive. In these civilian areas, the government has much less leverage, so that the relationship, the stick and carrot, that is available here is missing. It's an even more complicated issue.

Kelley: The last one I'd point out is this technology turnover. Just by the virtue of the speed with which we see change going in,

it's very difficult to achieve interoperability, because as soon as anybody reads about a new technology, especially during the hype phase, the next thing is I know I will see messages coming out explaining how dumb we are that we're not already on it. That's why I'm having Dawn Hartley put out messages saying, "No, we're not dumb. We're looking at all this new technology and we're in fact going to take care of it when it comes out."

We talked a lot about interoperability. If standards aren't enough, what do you do? The common operating environment (COE) is the next step beyond standards (figure 40). This is a set of rules that we give out to the contractors who develop our applications. We're essentially doing what Bill Gates does at Microsoft. With Microsoft, which is a proprietary system, Bill Gates sets the rules, and thousands of people develop applications that can run under his operating system. We've taken that same approach in the UNIX world and said, "Hey, here are the rules that we're going to use out of this UNIX thing. If you want to develop an application for me, follow these rules. Don't use this memory space here because you'll clobber the ATO." We divide up the space in the computer so that these applications can come in and interoperate, or at least peacefully coexist. Then we define other levels of interoperability above that where they can not only coexist, but also share information and work together; where there's total integration. This is a big step beyond standards, though. It's standards based, but it's taking it to the next logical step so we can get away from that problem where the standards are not perfect enough.

This is a good graphic that can talk to the NATO issue, which is where we are today (figure 41). When we talk interoperability, typically we get the least common denominator. I agree that interoperability is not just technical: it's procedural, it's operational concepts, it's that whole panoply of things. But in the technical arena, we get together, we meet at NATO, and we develop a box that will allow the different services and NATO things to talk to each other through very thin lines. But I would suggest to you that this model for the 20th century is not going to work. When you want to operate in the 21st century, you had better be fully integrated at

¹⁰ See Mr. Daguio's presentation in this volume.

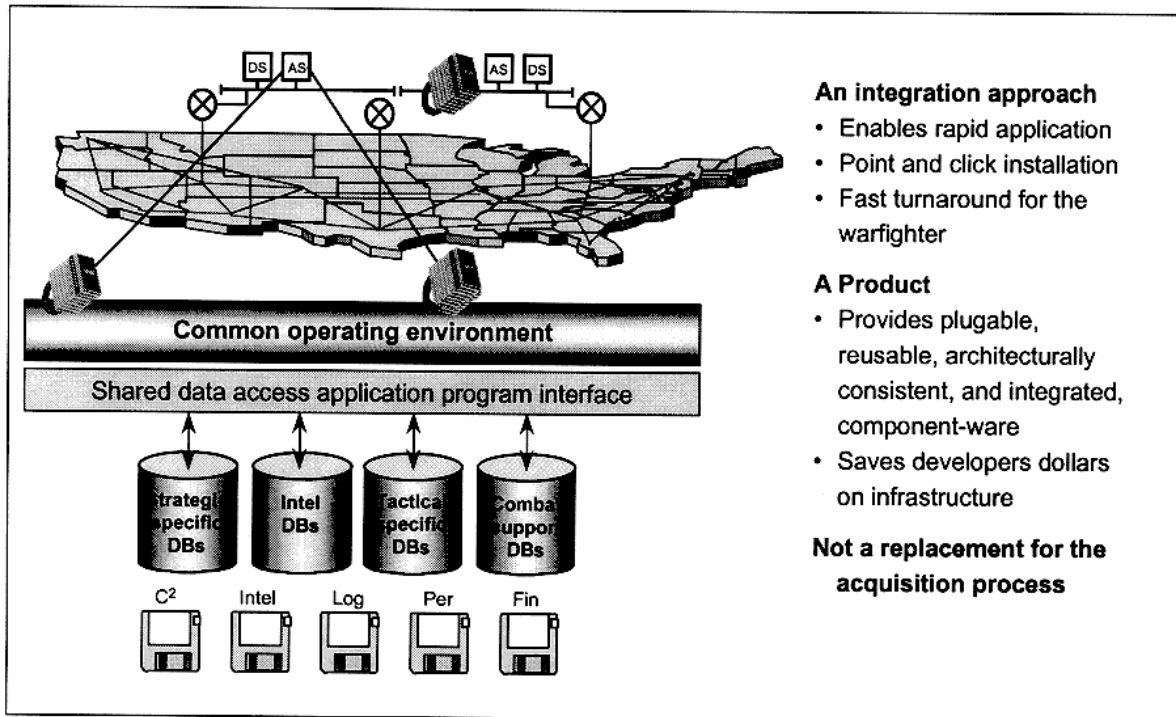


Figure 40
Common Operating Environment (COE)

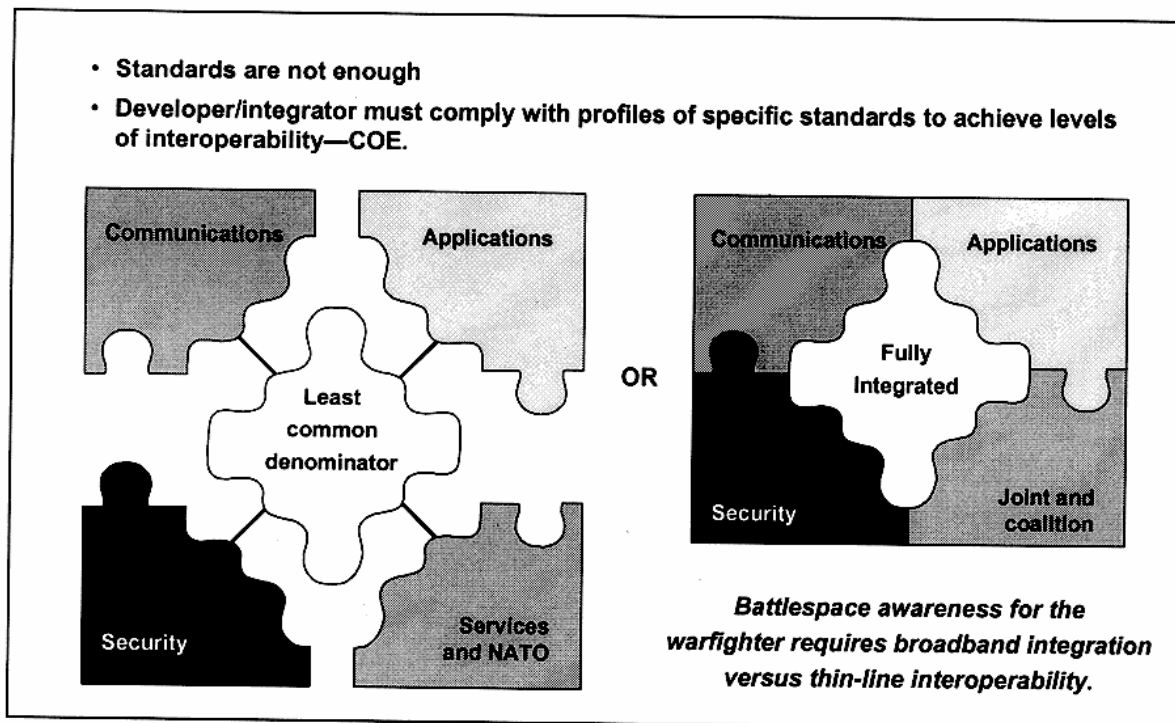


Figure 41
What Level of Interoperability Do We Want?

broadband so that you can exchange air pictures: who's attacking, where are they, who's coming in, where are the friendlies? Those are broadband-type applications that have got to be done. We need broadband interoperability.

This is just one example of interoperability (figure 42). There's a lot of hype on PKIs going on right now. In January, *Network World* published a big article about how all the vendors have agreed to interoperate. Do you remember UNIX? How many times have they agreed to give you one version of UNIX? There are 40, and probably 100, commercially viable versions, not including Linux, which is now floating around. That is another one we get letters about: "Why haven't you gone to Linux?"

"The declarations from vendors that they will support PKI interoperability, even as they compete fiercely, comes none too soon."

Remember UNIX!

*Source: *Network World*, 25 January 1999, p. 17.

Figure 42

Promises, Promises: The Myth of Standards

This is from General Zinni (figure 43), the commander in charge of Southwest Asia. We always like to have four-star generals say things like this, especially Pete. He likes to see people telling his command to start moving in and doing this.

"We are seeing USCENTCOM forces transition more to common systems and away from stovepipe systems that heavily tax our limited theater bandwidth."

General Anthony Zinni,
USCINCCENT

Figure 43

Supporting the Warfighter

Sort of by way of summary, this is our strategic focus (figure 44). I'm focusing on products, on getting things out to the warfighters. Pete's acquisition of GCCS took 2 years instead of 10 or 15, which is what it took to get the predecessor system out there. We're starting to get these products out by backing away from the traditional model that gets us an aircraft carrier, a bomber, or a tank. We can't use the same acquisition model when the technology in our business is revolving every 18 months. So we focus on products, and these are the kinds of thing we want. We focus on the customer. Our number one customer is the warfighter, but we have a hell of a lot of people who support them behind the scenes.

We've talked a lot about security, and defense in depth. We're trying to build it into the products now. With that COE, we're also putting security requirements in it for people who bring applications to us. So, over time, if people follow the COE, they will get more security, they will get guaranteed interoperability, and we'll have a way ahead, and guess what? We can then exchange applications among services. Right now, typically, a contractor will sell one thing to the Air Force, and sell the same thing to the Army, the same thing to the Navy—slightly modified, I might add, for each one of them. We're getting to a point now where we can avoid that.

I had to have one quotation in this briefing (figure 45).

Oettinger: Let me, if I may, capitalize on that as well, because we are fortunate in having not only General Kelley with us, but a number of his predecessors, going back to General Lee Paschall, have also come before the seminar.¹¹ And so, we have a rich record for you guys to exploit on the continuity of the evolution of these issues as the world picture, and the technology picture, change.

¹¹ See Albert J. Edmonds, "Information Systems Support to DOD and Beyond," in seminar proceedings; 1996, and "Integrated Information Systems for the Warrior," in seminar proceedings, 1995; John T. Myers, "Future Directions for Defense Communications," in seminar proceedings, 1989; and Lee Paschall, "C³I and the National Military Command System," in seminar proceedings, 1980.

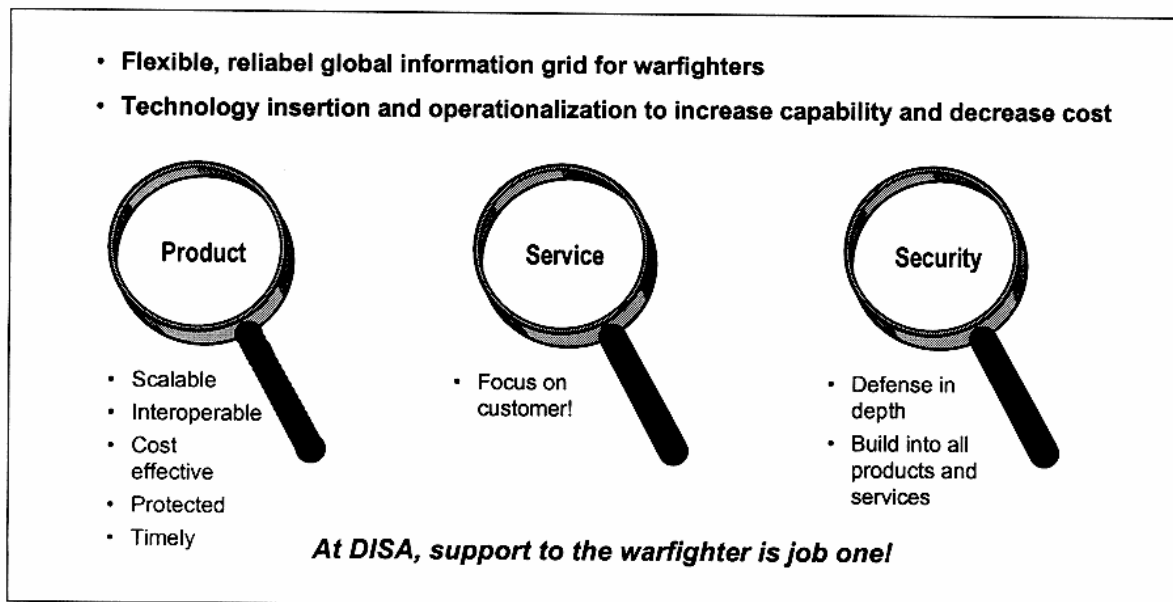


Figure 44
DISA's Strategic Focus

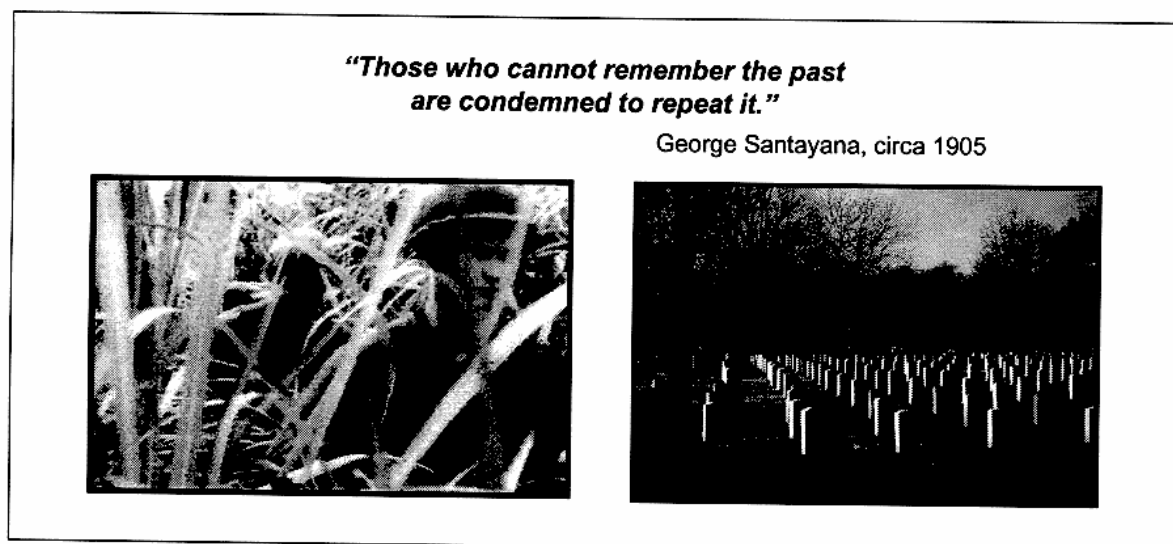


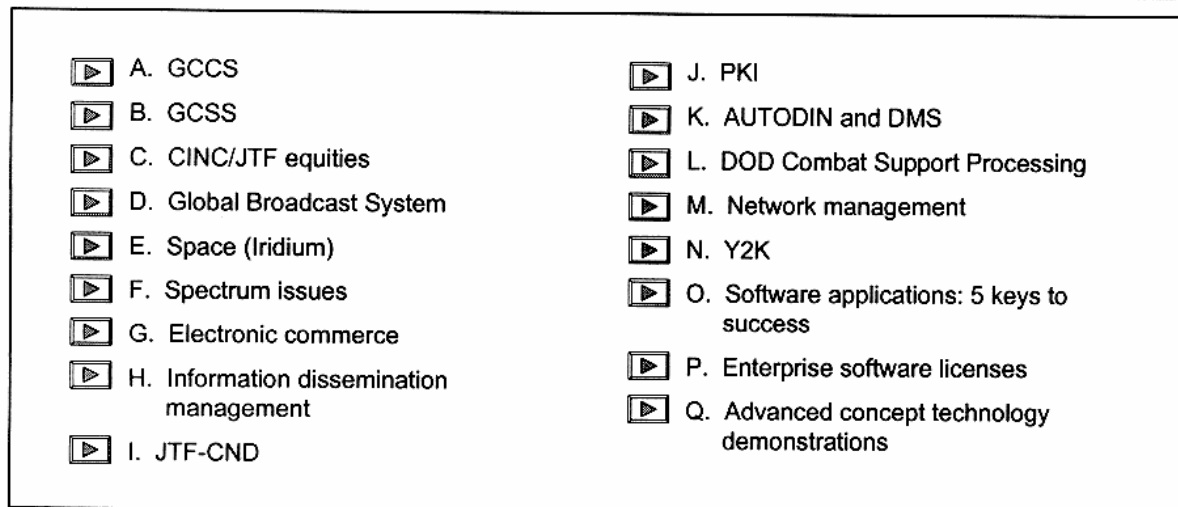
Figure 45
Conclusion

You can use them as a window to understanding this list of problems.

Kelley: You can use them as a consistency check. History gets distorted, big time.

Oettinger: Circumstances change.

Kelley: Circumstances change, that's right. These are just some of the things we're working on (figure 46). I'll be happy to talk



CND = Computer Network Defense
DMS = Defense Message System
GCCS = Global Command and Control System

GCSS = Global Combat Support System
JTF = Joint Task Force
PKI = Public Key Infrastructure

Figure 46
Menu Items

to any of the topics on this menu or anything else. I mentioned some of them; for instance, that Iridium's coming up.

Oettinger: Could I ask you to say a little bit about Iridium? Colonel Hays, our national security fellow, is working on a paper looking at the impact of some of these mobile satellite-based systems.

Kelley: I would be happy to. Iridium is the first one that's gotten into space. They have 66 satellites up. A lot of people don't know that Iridium has a low data rate, only up to 9.6 kilobits; most of it is 2.4 or 4.8 kilobits per second. That's barely voice quality, but the beauty of Iridium is that it's globally available. If you're on the North Pole, if you're in the Iditarod in Alaska, you can pull out your Iridium and call for a cheeseburger at the next stop. From a military standpoint, we're very interested in that. We go to some weird places. We have submarines that go into strange locations, and we're working with antennas and so forth so that we can in fact use Iridium for global coverage in these areas.

On humanitarian missions, this would be a very useful technique for the initial forces going in, and for the nongovernmental or-

ganizations, which we discussed earlier. When you go into Rwanda, where there's no infrastructure, this kind of capability would be very useful.

What we are in fact doing is getting secure handsets. We want to avoid the Jimmy Carter syndrome. If you remember, when he went to Haiti and negotiated the treaty there, we had the folks ready to fly, to jump in and do a forced entry. He came back on the airplane and said, "Hey, I've got an agreement, and here it is." He read the agreement on the airplane, and the agreement was on CNN before it got back to Washington. So we want to sort of avoid that.

Oettinger: Just to be politically correct, that used to happen to Ronald Reagan also.

Kelley: That's fair. Now we've got a Democrat and a Republican.

Student: Sir, do you see any relaxing of the requirements for assured access and that kind of stuff for the military for combat service support so that we can move into these other satellite systems that are offering access?

Kelley: We're doing a study on Ka-band right now to take a look at that. Assured ac-

cess for the logistics community is important because typically in a battle, whom do we first throw off the telephone? The log community. We figure that the bullets are on a boat, and they're going to get there when they get there, and we'll take them off then. But I think we have a way to assure access with the Global Broadcast System (GBS) and a few other things coming down, and if the log community is clever, they will get involved in that. That's why we're working so hard on GCSS.

Paulson: The J-4 is probably the biggest supporter of the teleport concept, where we now put commercial bands into our ability to project, because he knows that's his means of getting availability on the comm system.

The down side of Iridium, right now anyway, is cost. Right now the handsets cost about \$3,000 each. They also have a monthly fee that runs \$100 or \$150, but your usage usually averages about \$7 a minute, so that's fairly expensive. That will come down with usage and other competitive things being put out there.

Kelley: When GlobalStar gets out, we expect Iridium prices to drop significantly. But right now, they're the market-share king, so they can charge what they want to.

Paulson: We invested in our own earth station, by way of Iridium, so out in Hawaii we have an earth station and all DOD calls go through that. That's another security piece of this. It gives us the ability to protect who is making the call.

Oettinger: Ladies and gentlemen, we have about three minutes left, so it's your last chance.

Student: Could you address information dissemination?

Kelley: In three minutes? I'm glad we held that for the last, and have only three minutes on that one!

It is a big issue. When we put the GBS out in Bosnia, which was when we first did

this, we had 24-megabit pipes, 6 megabits, and so forth, and the first thing we ran into was that we all of a sudden became TV producers. We had to figure out what would go on this channel and then, by the way, where is the source of the information? We're working with the Defense Advanced Research Projects Agency on developing software tools, a little bit like Web search engines, that can be used to go out and query the CIA, the National Imagery and Mapping Agency, all these different databases, and try to bring the information back. But we've got to get some sort of a quality factor on the information. How do you know that the information you've got is the latest, and that kind of thing? So there's a whole host of dissemination issues, of quality factors, of sources, and of tools to be able to load that broadcast automatically. So that's what we're doing in dissemination.

That's just for the broadcast. Clearly, information dissemination is much larger than that. With this whole host of things we've been talking about today, all of it has a piece of information dissemination involved in it.

Oettinger: Let me relate this to another thing the general brought up earlier with the ATO: that whole question of supply push and dissemination versus demand pull. The ATO looks very different depending on whether you push information out or ask somebody to let you pull it down. You've opened up a large set of questions.

Kelley: It's a fertile field for creative minds to be working at.

Oettinger: However, we have run out of time at this session. I want to thank you so much for everything. We have for you a small token of our large appreciation, and we'll get one for Pete too. I just didn't know he was going to be a part of the seminar. Thank you.

Kelley: Thank you, I enjoyed it. Good luck to all of you.



INCSEMINAR1999



ISBN-1-879716-63-1