INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Integrated Information Systems for Warrior
Albert Edmonds

Guest Presentations, Spring 1995
Michael L. Brown; William A. Owens; R. C. M. (Mark) Baker; Arthur V. Grant, Jr.; A. Jay Cristol; Robert Lawrence; Albert Edmonds; John A. Leide

January 1996

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-29-1 **I-96-2**

Integrated Information Systems for the Warrior

Albert J. Edmonds

Lieutenant General Albert J. Edmonds is Director of the Defense Information Systems Agency, and Manager, National Communications System, with headquarters in Arlington, Virginia. He is responsible for providing command, control, communications, computer and intelligence (C4I) support to the nation's warfighters. General Edmonds entered the Air Force in August 1964 and was commissioned upon graduation from Officer Training School, Lackland Air Force Base, Texas, in November 1964. He has held many critical C4I positions, including Deputy Chief of Staff for Communications-Computer Systems, Tactical Air Command (dual-hatted as commander, Air Force Communication Command's Tactical Communications Division); Assistant Chief of Staff, Systems for Command, Control, Communications and Computers, Air Force Headquarters; and Director for Command, Control, Communications and Computer Systems Directorate (J-6), the Joint Staff.

Oettinger: I take great pleasure in introducing our speaker this week, who is back with us, which is a great delight. He was with us last year in his capacity as the J-6. He's with us this year in his capacity as the director of the Defense Information Systems Agency. You've seen his biography, so I won't go into more detail and eat into his time. I'll just let him go ahead. It's a pleasure to welcome you back, Al.

Edmonds: Thanks, Tony. Let me just tell you that I'm going to go through a little bit of history—about two, three or four minutes of it, and then I'm going to introduce you to some acronyms. We would not be military if we didn't have a lot of acronyms. I'll also tell you what they are, and won't use them as much as you think I would.

The first thing I want to talk about is the easiest thing to talk about, C4I for the Warrior (figure 1). I'd kind of like to update it. It's a review from last year. I'm going to tie this to the current initiatives, and then talk about future directions. Please break in, interrupt, and ask questions. Say, "What is it you're talking about?" Don't let me get to the end and then say, "That thing back at the beginning of the briefing ... what were you talking about?"

This is my purpose (figure 2): to tell you how I'm going to deal with support to the warfighter—the joint warfighter, and I might add, coalition warfighter, because we very rarely would go to war again just on the basis of the Marine Corps fighting somebody. We're going to be helping

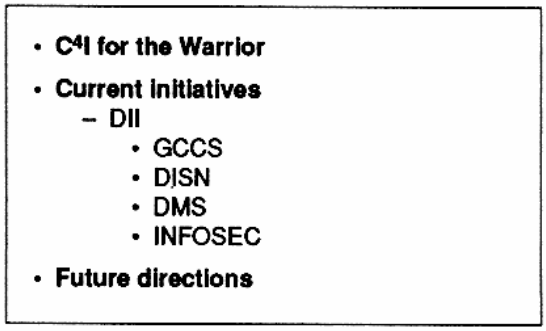


Figure 1
Overview

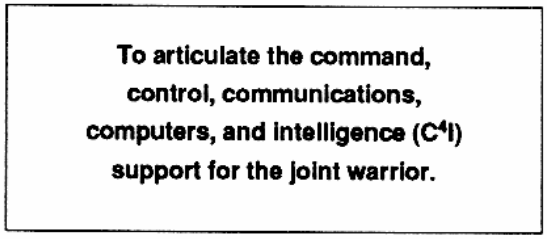


Figure 2
C4I for the Warrior: Purpose

somebody else, I hope, because we're not planning on doing that here in the United States.

Let me orient you on a little bit on what I do and what I did with our organization (figure 3). This is not an eye test. Tony mentioned that I came from the Joint Staff J-6. When I got to the Defense Information Systems Agency (DISA), I found a lot of different kind of organizations, like D&GO, D&GA and that stuff, that were acronyms for things like Defense something Operations, Defense something Acquisition. Since I got all these things like special staffs, the first thing I did with the agency is divide of all the headquarters functions to do policy and resources. The two lowest rows in the slide are field activities that have special kinds of meanings, like DISA Europe helps the CINC in Europe, DISA PAC helps the CINC in Hawaii. JITC is a testing center. DITCO buys stuff. WESTHEM (Western Hemisphere) takes care of the continental United States. The White House Communications Agency (WHCA) has about 1,000 people who support the President and Vice President and emissaries, and they take care of all the communications, automation, audiovisual, picture-taking, public address, lights for the Christmas tree at Christmas time—you name it, they do it all. For each one of the CINCs I have a slot to give them technical support and engineering support. And these are my countermeasures guys, my security and information warfare people, the Joint Spectrum Center (JSC), and some contracting people.

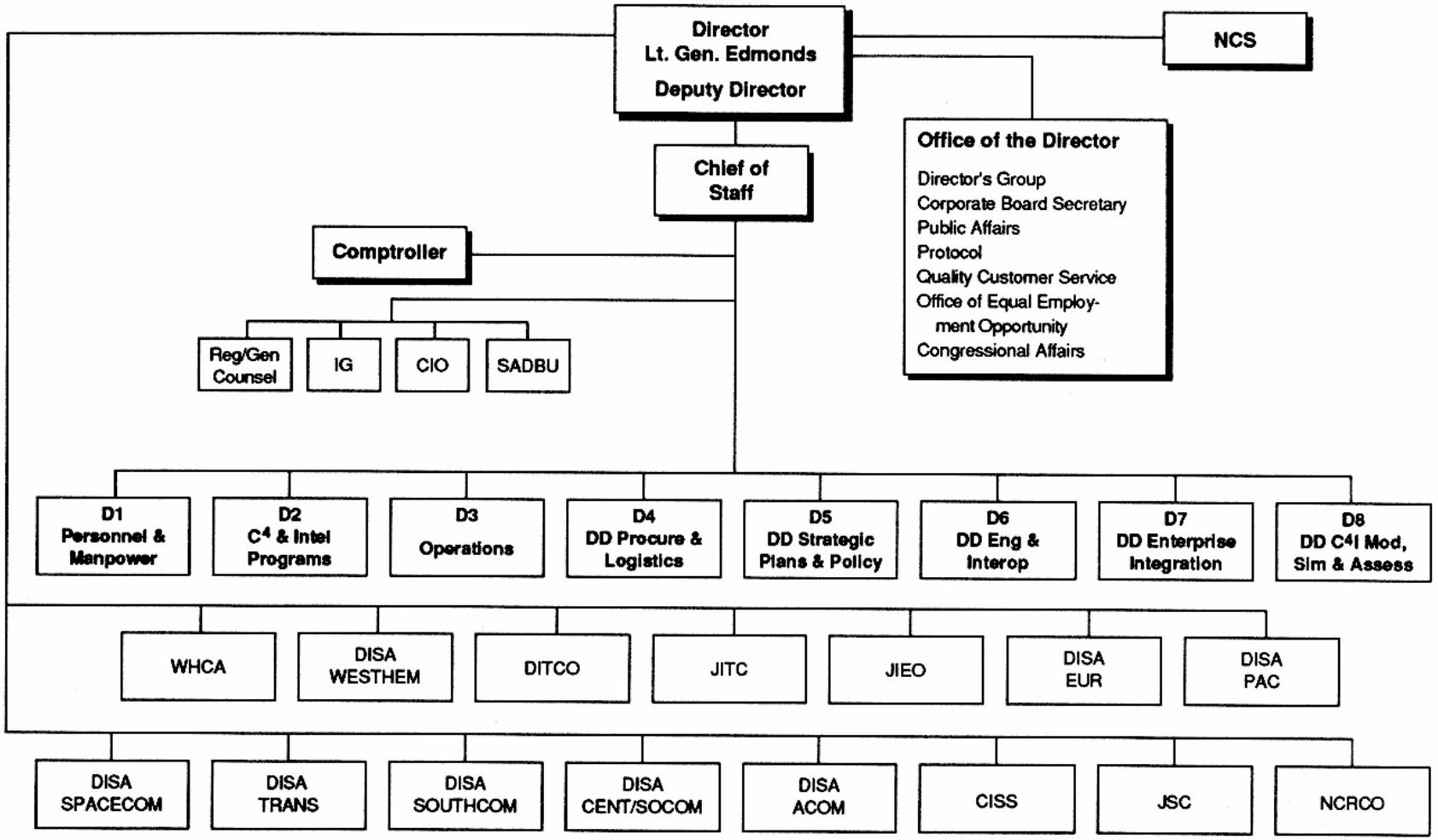
The most important thing about this chart is that I try to make sure that the warfighters are going to stay in my organization by numbering them like the Joint Staff—D-1 through D-8. D-1 is personnel and manpower. D-2, since I don't have much intelligence, I call intelligence and C4 programs. D-3 is operations, like G-3, like J-3; D-4, procurement and logistics; D-5, strategic plans; D-6, engineering output and interoperability; D-7, enterprise integration; D-8, modeling and simulation, like J-8. So I try to organize like the Joint Staff so that the CINCs and the warfighters can say, "Mmm, that's my counterpart."

Now, let me give you another bit of orientation about this (figure 4). DCA was the Defense Communications Agency, and this is the Defense Information Systems Agency. Back in the 1960s, we did secure voice, regular voice, a message system called AUTODIN, a red HF (high-frequency) network worldwide to help airplanes fly around the world with mostly position information, and the Worldwide Military Command and Control System (WWMCCS), and we did engineering for all this stuff. It was a very easy job, involving about 3,000 people.

In the 1990s, they threw all this stuff over the fence to us. Almost all these systems now are being modernized with new digital technology. In addition to that, new things have come on the horizon, like video teleconferencing and huge data processing centers. We took 157 of them, and brought them down to about 16. Joint spectrum means managing frequencies. We auctioned off some frequencies in this country to raise money, but when you go overseas, the frequencies belong to the sovereign countries. So how are we going to do frequency management in a war environment? I talked about information security and architecture items. The main thing is that we're changing to the virtual 2000s with a dynamic "Global Grid," parallel C4I operations, and integrated intelligence, customized service for the warfighter any time, any place, any nation, sensor-to-shooter.

It's very difficult to define all this stuff to people. I grew up with fighter pilots, and we showed them pictures. This again is not an eye test (figure 5). I want to get the perception over to you that the Defense Information Systems Agency can look at some of these things on this chart. On the bottom here are those things we do for the whole Department of Defense as part of our infrastructure support. We do testing, we develop standards, we do modeling and simulations, we do security, we do architectures. We do these things for everybody. It's part of opening the door.

I'll come back to this part of the puzzle. This is cross-functional, cross-service integration between logistics and operations, intelligence and operations. We have the responsibility for that kind of cross-



ACOM = U.S. Atlantic Command
CENT/SOCOM = Central/Special Operations Command
CISS = Center for Information Systems Security
DISA = Defense Information Systems Agency
DITCO = Defense Information Technology Contracting Office
JIEO = Joint Interoperability and Engineering Organization
JITC = Joint and Interoperability Test Command
JSC = Joint Spectrum Center
NCRCO = National Capital Region Contracting Office
WESTHEM = Western Hemisphere
WHCA = White House Communications Agency

Figure 3
DISA

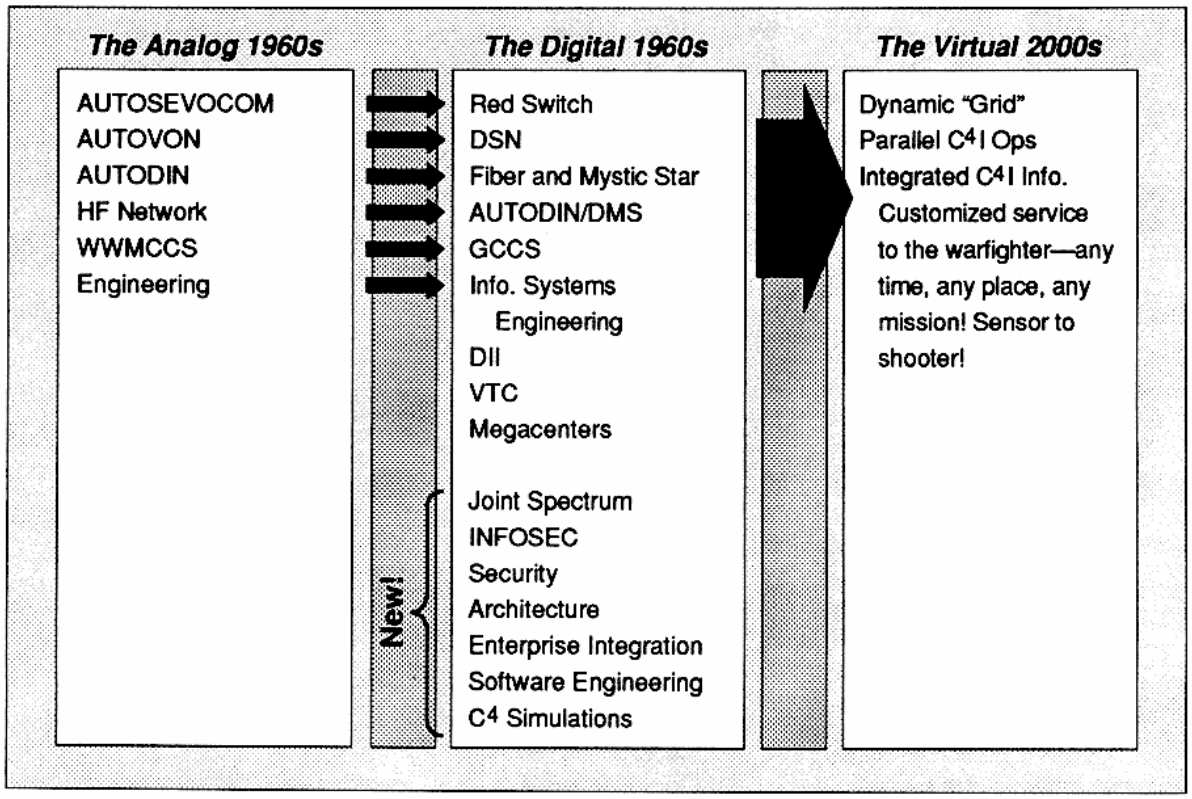


Figure 4

DCA to DISA

functional integration with the functional people. We do the technical part.

We do enterprise integration for the Department of Defense. In those megacenters I talked about, the big data processing centers, we provide shared mapping data into those command and control systems for command and control applications and intelligence applications. There's a lot of hardware involved, but this is primarily software integration that I'm talking about, not hardware. Base and tactical applications means some of those things that it takes to run a post or camp or station, whether in peacetime or wartime. Mission support is things like finance, personnel, and those kinds of things that we need to support the warfighters. I put "future services" here because whatever I don't have up here, someone will say, "You forgot my piece!" and I say, "It's right here!"

A very critical piece here is electronic commerce (EC) and defense messaging. Electronic commerce is a very big, growing concern. We order a lot of stuff in the Department of Defense and sell it to commercial people. But most people pay with paper: vouchers and checks. More and more this is going to become completely electronic. Electronic data interchange (EDI) involves sending tech orders, tech manuals on how to maintain a ship, how to maintain a computer, how to maintain a typewriter. Those things are going to be transmitted, or they exist on the World Wide Web. So if you want to know how to maintain your PC, you find your PC on the World Wide Web, you go to maintenance, and you tell them what the problem is. You can get a lot of that electronically. So we are providing the infrastructure for that, the communications lines and some of the computers to help process electronic commerce. Right now we order all of our foodstuffs for the commissaries electronically from General Foods. The problem is we haven't got the other part done yet, so that we can pay them electronically.

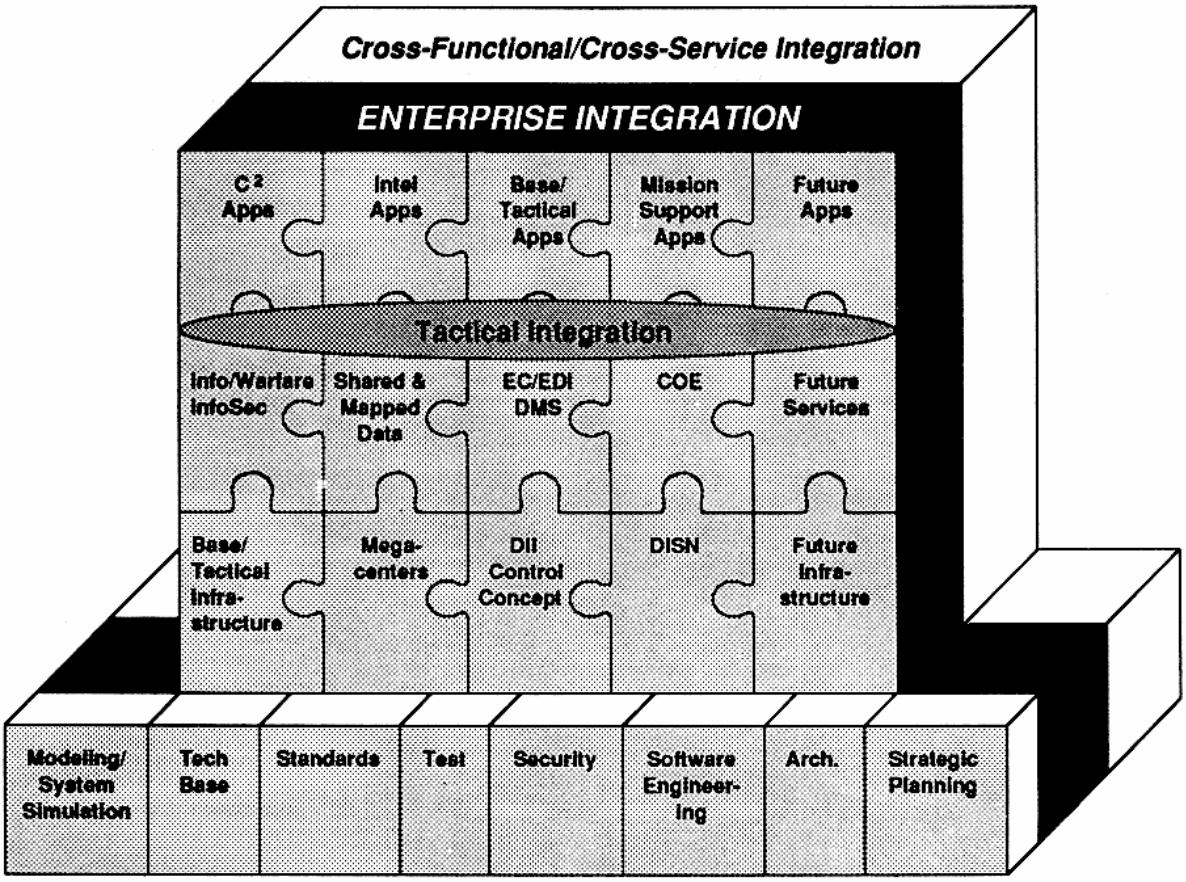


Figure 5
Elements of the DII

Oettinger: Just to tie this to sort of my understanding of the past, some of these functions are functions that must be newly under your wing. They were the kinds of things that Strassman was talking about in the simulation environment. Can you say a word about when this migrated into what is now DISA?

Edmonds: What has happened is cross-function and cross-integration. For example, this electronic commerce function belonged to the procurement people in DOD, the people who are responsible for buying things for the Department of Defense. But they can't do anything with it independently. So they've come to me, and we've created a team of my people and their people. I provide the computer processing and communications part of it, and they provide the functional software that says "What do I need?" So we took the function of procurement, and, as a matter of fact, we're buying a commercial off-the-shelf software product to load in our computers to let us buy stuff. I provide the hardware and software support and the communications to allow that to happen.

Another example: in these megacenters—they're humongous things—there's logistics data, finance data, medical information, all being processed here remotely, and pulled from different sites—from as far away as Korea or Saudi Arabia. All of the Army's supply support for the Patriots in Korea comes out of a megacenter down in Huntsville, Alabama. DISA is running that megacenter and providing that service to the Army. This is part of the things I showed you that got thrown over the fence.

Another example is this common operating environment (COE). I'll talk about that when I talk about the Global Command and Control System (GCCS). This COE is

a bunch of technical things available to all the people in the Department of Defense. If you build your system using the COE, with these standards, on this architecture, theoretically it will all work interoperably with everything else. We'll test it to make sure it does. That's the combination now.

You see I put a little oval on the slide called tactical integration. This is very important. There's a constant debate on what's strategic and what's tactical.

Student: Sir, on this common operating environment, I'm trying to reconcile that with something Admiral Owens spoke to us about, which was interoperability. If you look at the armed forces in the United States, in the left-most column you can list a myriad sensors, and in the right-most column, you can list a myriad delivery systems or weapons systems, and in the middle you have C4I.

Edmonds: I get the picture already.

Student: So what he wants to happen is that no matter what sensor you use, currently if you use sensor X, you can only get to delivery or weapons systems Y and Z through C4I. He wants to get to the whole alphabet with that sensor. My question is: does your common operating environment at all relate to that?

Edmonds: Yes, and I'll show you on the chart how that works. As a matter of fact, if you take this piece right here called DISN—that's the Defense Information System Network—it is supposed to be such that you can pull information any time, anywhere, from any sensor, to any shooter. That's what Admiral Owens and I have been dialoguing about: how to make sure I've got the capability in here to allow that to happen using these standards, the common operating environment, instead of the elements. (I'm going to talk about all three of those.) When we put the three together, it ought to happen seamlessly.

In the past, nobody ever told me to do this enterprise integration. DISA has never had that job before. Nobody had that job. We did it on the fly. We got it and we said, "Woe is me!" I have the EC-2, E-2C, and the E-3. I have TRAP (Tactical Related Applications Program). I have U-2s. I have KC-135s. I've got all this data. Everyone has their own ground processing center. When you get it all in one place, it's called a fusion center. You've got about 800 people there trying to put it all together and hope you get a product somebody can use. We're going to get rid of that.

That's why this intelligence application is right here in the top row also, because this is the same thing as the sensors. If you take this common operating environment, use this transmission medium, this messaging medium, based on these standards, and the architecture we have over all, secure it however you need to, you can model it, make sure it looks good and feels good. Then you test it and do it.

Oettinger: When I hear his question and your answer I think I hear—but I'm not sure—some relationship to some of the things that we heard over the past couple of years from Jerry Tuttle.* Am I right or wrong?

Edmonds: Exactly, you're right!

Oettinger: ... so that conceptually what you're doing is extending the implementation of some of those ideas that he expressed here about what he was doing in the Navy. Is that right?

Edmonds: Absolutely, not only conceptually. Let me show you this next chart and relate to it.

I take the same thought process I just got through about interdependencies here (figure 6). What I basically do is take operations and put it in command and control.

---

* Jerry O. Tuttle, "Tailoring C3I Systems to Military Users," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1988.* Program on Information Resources Policy, Harvard University, Cambridge, MA, March 1989; and "The Copernican Pull," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1993.* Program on Information Resources Policy, Harvard University, Cambridge, MA, August 1994.

I don't break out intelligence as a separate thing, because one of the jobs I had in the J-6 was forcing C4I for the Warrior, not C4 *and* I. So I look at it as operations.

You'll notice all these things here are the other functions that support the warfighter. Base/tactical infrastructure is what you have on posts, camps, and stations. But all these things in the lower right-hand circle are what I'm bringing to the table now—the common operating environment, the DISN (the information system network that I told you about), the modeling systems. I have standards. We're doing software engineering, we're testing the stuff based on its architecture. This is our enterprise infrastructure.

In his Copernicus architecture Jerry Tuttle tried to take a lot of Navy systems, all kinds, and he said, "Okay, I see 10 different intel systems. I'm going to take all of those and boil them down into one." That doesn't mean he got rid of all the applications when you do that. Out of those 10 you might have seven of those applications left, because you can only throw away three. You put your money on making those seven better. If you make those seven better, then you have about three of those things left, because four of them go away. Those things become very robust. But also you get them by using good software engineering techniques based on these standards—this common operating environment—and now you've got something to plug into all kinds of systems. Basically, that's what we've done. I'll show you something that we evolved that to in a minute.

Now let me show you another picture of this same thing (figure 7). It's important to show it about three times. Let me tell you why. Because, in working this problem, you don't deal with just the operators, or

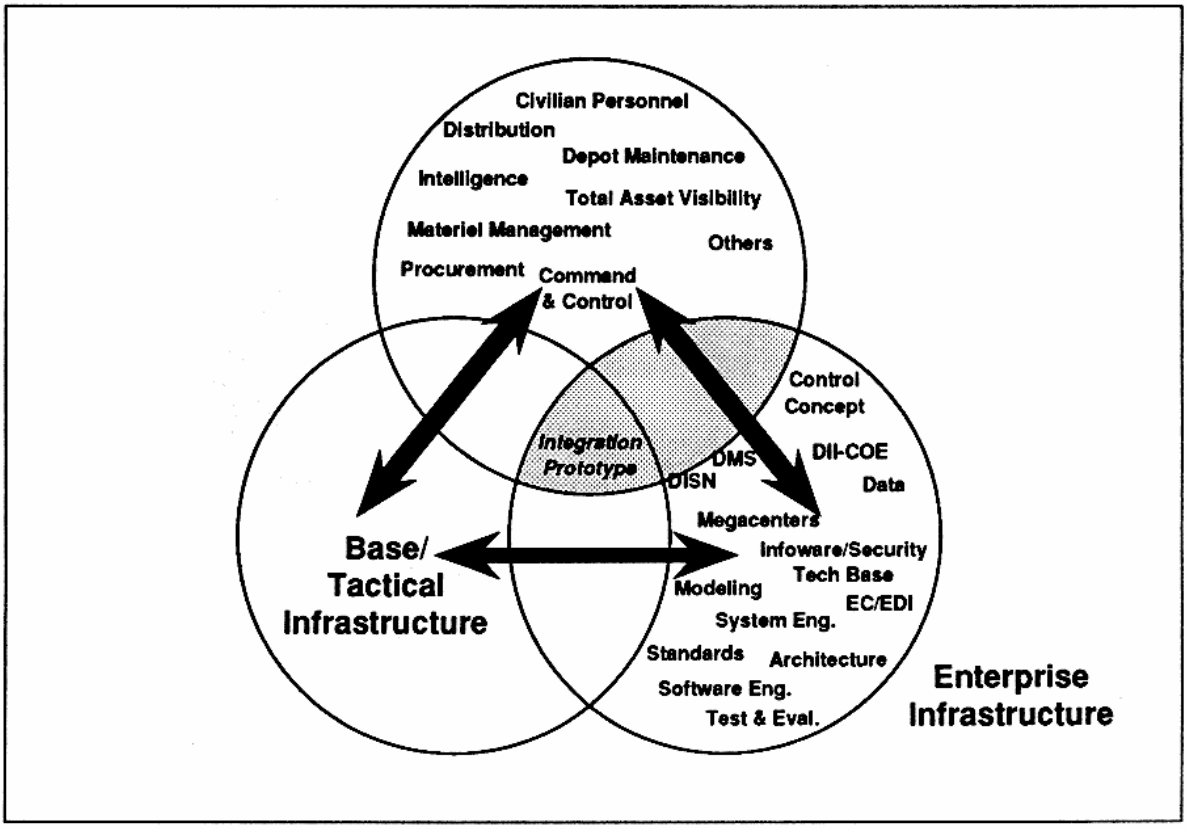


Figure 6

DII Interdependencies

just the technocrats, or just the resource folks; you deal with the money people. The center is DISA. I keep showing you standards, architectures, integration, and testing. This band of Enterprise Integration, though, shows you the commonality, or the togetherness, or the teamwork that must take place for this to happen. I can't run these things out here. I'm responsible for things like architecture, test and evaluation, and standards. But this part, like EC/EDI, belongs to the acquisition people. Mission support belongs to finance, and personnel belongs to them. Intel belongs to intel folks, but together, we are going to integrate this enterprise using these tools.

The reason why this is important is that I want money from them. How am I going to pay for this stuff? Then I do my part. Also, I've been given this job in the white area of the slide to help integrate it. I have teams working with almost all these people. I have from 8 to 20 people from each one of those folks to do that integration. Now, how do you capture this to do this thing and make sure you don't lose it?

Oettinger: Before you go on to the next slide, could you go back to that one because I want to ask you a question again to tie this to some other things. There is a large literature out there, including some books by a fellow named Paul Strassman, who at one point was the sort of information management guy in the Office of the Assistant Secretary for C3I. As I read the record, what happened under that regime in following those ideas was that you created

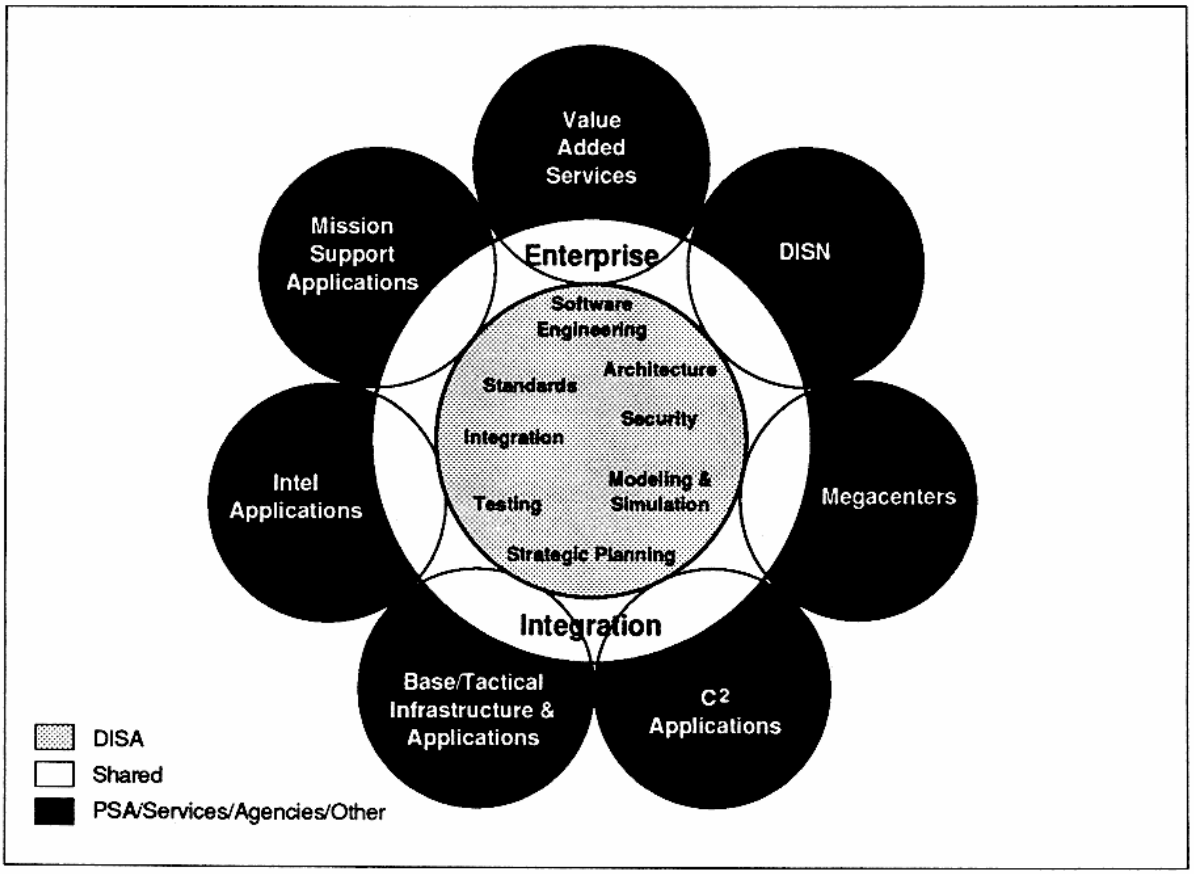


Figure 7

Notional View of the DII Funding Strategy

a great deal of resistance and nothing happened, because it seemed like sort of a top-down thing. Yet if I hear you, you seem to be heading in the same direction, but by a more consensual and cajoling and ride-on-their-backs and get-them-to-do-it process. Could you comment on that? I may be dead wrong, but ...

Edmonds: What Paul did was correct. He tried to get the functionals—I call these folks functionals: the functional advocates, the procurement people, the logistics folks, the finance, the personnel, who are in the Office of the Secretary of Defense (OSD) and are responsible for those functions for the department; I put them in the value-added services to these guys—to improve their processes. What he did correctly with them was come up with a fund called the Simulation Central Fund to give them some money to go in and improve that process. So if you did logistics all your life, and you thought it was okay, but you didn't improve it, he gave you some money to get some outside people to come in and show how they can do the process better. He also gave DISA and these folks some people to help them do that. These are technical people as well as functional people.

Those people still exist. But what we try to do, rather than sit over here and give them a technical solution—issue it to them—is build teams, like with the EC/EDI folks. I have about 30 people working electronic commerce. I pay the salary of about 20 of them. They are technical. They're computer people. They're communications people, but they're also people who know how to do electronic commerce because they've been in procurement before. We're now putting this capability out in the Department of Defense and also the government. As a matter of fact, Secretary Shalala already hooked the Department of Health and Human Services into the backbone. The states of California and Oklahoma asked us to do the same thing.

Student: So basically, General, what you've done is created your own consulting agency.

Edmonds: Except we don't consult. We also work. As a matter of fact, what I tell people is: "I don't need any consultants, and don't tell me how to do it. Let's get together, roll up our sleeves and do it!" That's exactly what we do, because the consultants want to sit around, talk, and do studies. I've got a lot of money to go to colleges and universities to do studies for me. I don't do studies. You do. We do C^4 right.

So that's exactly what we've done. So we're trying to take this from a little different angle and be more consensual here with the group.

Now in Washington, I learned a couple of things. You've got to come up with some kind of way to institutionalize what you're doing, or when you travel on to the next place it's gone. So we came up with the DII master plan (figure 8). DII is the Defense Information Infrastructure, and so you won't get confused, there are a lot of "II"s. One thing you should know is that the IIs are the same: information infrastructure. There is the DII, which is defense; there is an NII, which is national; there is a GSII, which is government services; and there is a GII, which is global. All those IIs have some connection to the information infrastructure, and that's also the superhighways. They all have a purpose, they have a place. We do the DII right.

What we've done in building the DII master plan, for a couple of reasons, Tony, is also to institutionalize what you're saying. We have an overview, but in here we have DII elements—the same things I have in that puzzle back there: initiatives and opportunities. In that arrow (Section 2, DII Elements), you have baseline and migration initiatives. In the migration initiatives, what we've done in each of those functions—personnel, finance, procurement, logistics, command and control, and intelligence—is put a chapter or section in to tell us how they're going to migrate their systems forward for the future, either new systems, commercial off-the-shelf, or old legacy systems that they're going to modify, change, or whatever. I've told them that I'm willing to help them do that by doing some prototyping. I will take some of my money and help them prototype. So when

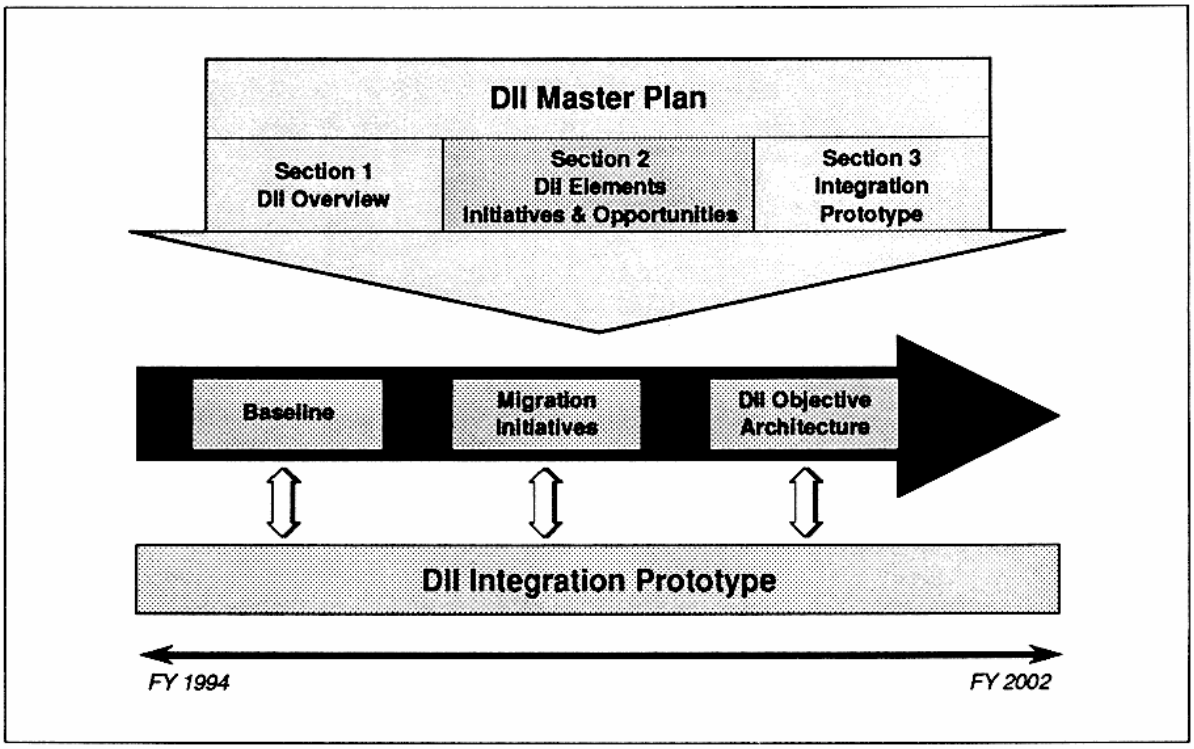


Figure 8

DII Master Plan

we do that puzzle down there, right now down at Warner Robins, we'll try to take some of those pieces and start tying them together to allow them to do cross-function and cross-service exchange of information between maintenance, supply, and finance. We're the ones who are going to help integrate that, without contract support.

At the bottom of the slide is our timeline to have a lot of this done. Since October 1994 we have upgraded two versions of this master plan, and in three months we'll have the third version. Why so many versions? Because when we first started folks didn't take us seriously. They didn't think we could do a good product. We did a good product in the first one, and then people got very excited. The second product was absolutely superb, and now people really have taken up this document, and this DII master plan has become part of the Joint Staff planning cycle that starts with the defense guidance. The program people in P&A (Programs and Analysis) and the Comptroller are going to take this master plan and see how the functionals are doing based on their plan in terms of funding things and making progress. It was a very important step for us because we were not in this cycle before. This was all the domain of the CINCs and the services and the Joint Staff. So we broke through with that.

In the next few slides I'm going to take that old puzzle that I showed you, and I'm going to explode a few of those pieces off that for you and talk about them a little bit and let you know how we do it. You've got to eat an elephant a bite at a time, you can't eat it all at once. So we're going to eat this elephant a little bit at a time, and we're going to explode these pieces. These are the pieces I'm going to explode for you today (figure 9): the Global Command and Control System, the message piece, the DISN piece, and the security/INFOSEC piece.

Now why those four pieces? Let me just give it to you in a nutshell. If I were king for a day and didn't have to do anything else, I would do that bottom piece of the puzzle because that's kind of like how

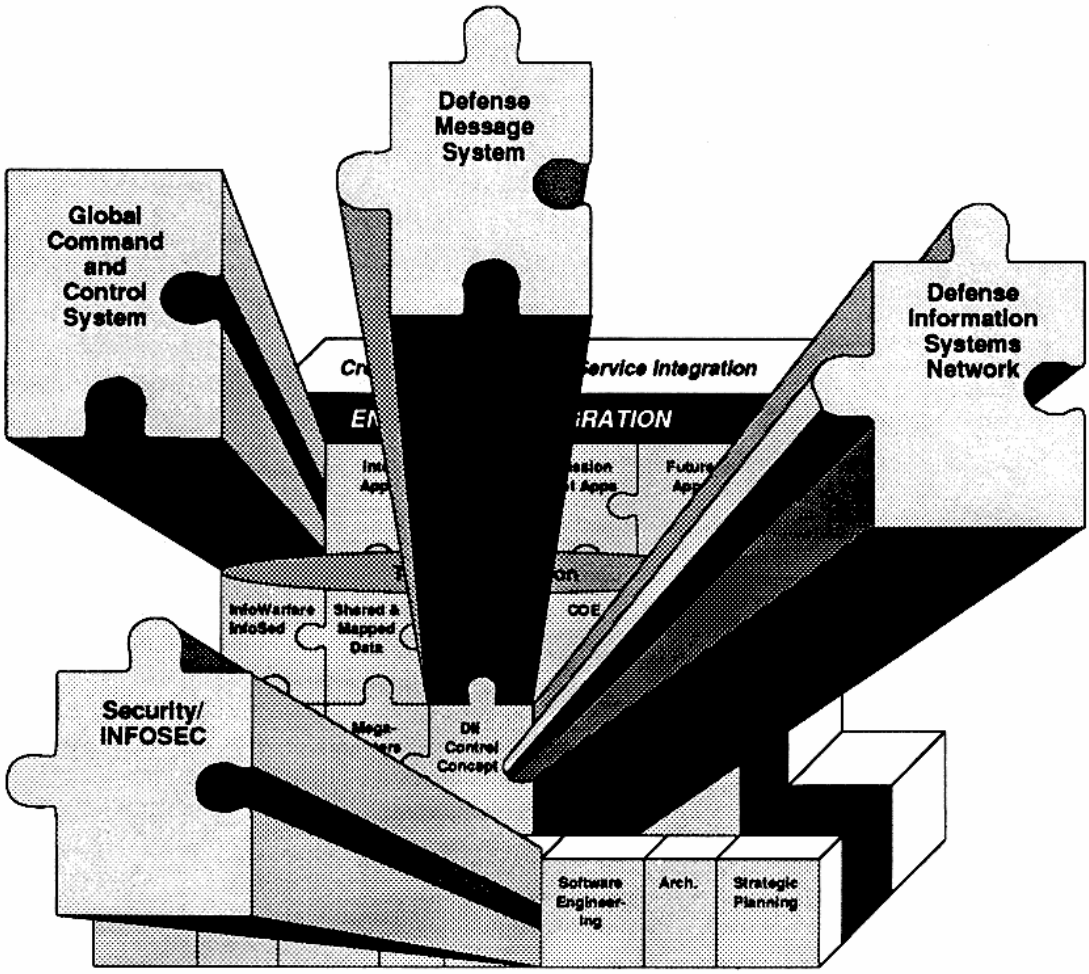


Figure 9
DII Near-Term Requirements

you open the door and build your house. But first is the GCCS piece, two is DMS—the messaging piece (and we save a lot of money when we're doing this one; I'll show you a chart on it), and DISN is the transmission piece. So you have command and control, messaging, transmission—very key pieces. This is why DCA, the old organization, existed before: to perform these three functions. Those functions still exist. We have to perform them as the baseline of what we do. We still have to do that right. But over here is a new piece: information security or information warfare. GCCS, DMS, and DISN must have a degree of security associated with them. So security now has become a very vital piece of what I must do as part of my baseline work. I must do security if I do nothing else. So I will talk about them very briefly, and we'll get rolling.

The first piece I'm going to talk about is GCCS, because that's the most important piece to me. I'm biased, because I did this at the Joint Staff. This is the mid-term part of C4I for the Warrior. Our quick fix was translators to take similar systems and make them talk to each other and exchange information. We did that successfully and, I might add, we declared victory in about 9 months. The mid-term was GCCS, and what we did is we took the Navy's OSS, Operating Support System—their joint maritime system—and we grew it to a joint GCCS. Let me tell you what our objective was (figure 10).

The Vision

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 10

Global Command and Control System (GCCS)

Oettinger: This, I presume, is sort of the successor to what used to be the WWMCCS and so forth?

Edmonds: It will be. That's right. As a matter of fact, that's a good point. On September 30, 1995, we're supposed to turn off the old WWMCCS (figure 11). It is a very expensive system, deliberate planning, no real-time command and control, and people hated it, but it was the only thing we had. It was a real mainframe computer-oriented system with a lot of security, and we couldn't share it with allies. So it's going to go away. This GCCS is going to provide that real-time, fused picture of the battlespace, the ability to respond and coordinate vertically and horizontally in that battlespace. That's what this system can do.

I can tell you right now that when we got ready to go into Haiti, I could sit in my operations center and the President of the United States, the Secretary of Defense, and the Chairman sat in the National Military Command Center in the Pentagon. We could see those 60 airplanes that took off from Pope Air Force Base all the way to Haiti, and we could see them when they turned around and came back, because we had a real-time picture of that battlespace.

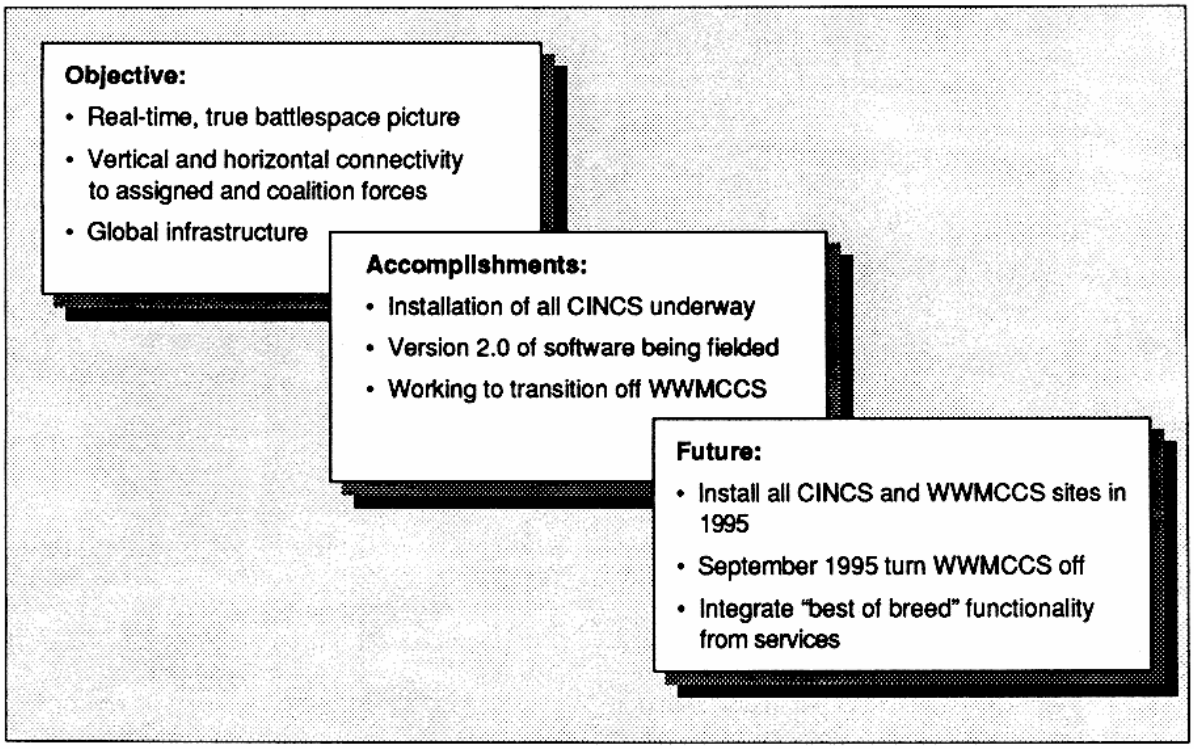


Figure 11

GCCS Is the Heart of C^4I for the Warrior

We could also see the combatant ships in the area. We could see them as if we were sitting out there, and they could see the same picture I saw. It took us 48 hours to put the system into the Pentagon. It took us 12 hours to put it in my operations center. It is absolutely that responsive.

Student: Sir, we have 10,000 questions about what you said, but one example is that General Shelton* was here a couple of weeks ago and talked about some of the high-level phone calls he got in his Hum-Vee on his MSE (mobile subscriber equipment), and he was amazed by all of that because a lot of it came from the White House. He was just surprised at the connectivity.

I have two questions. I hope I'm in the right realm here. There was something called the Joint Task Force Advanced Technology Demonstration and Advanced Concepts Technology Demonstration—ATD and ACTD—and ARPA (Advanced Research Projects Agency) is doing a lot of that. Are you involved in those demos, and if so, how?

Edmonds: ARPA and DISA have a joint program office designed to do technology instruction for all of this stuff we're talking about, and we have a quarterly review of all the projects and things we do. We also have had a Joint Warrior Information Demonstration every year in August or September for the last three or four years. The Army was doing it for three years while I was in Joint Staff J-6, and I liked it so well I took the program from the Army. It was called STND—Secure Tactical Network Demonstration—and I called it Joint Warrior Information Demonstrations. A CINC sponsors it every year (CINCPAC is sponsoring it this year) and a service is the lead service for each one of them. We take this very technology, the very concepts we're talking about, and we demonstrate the ways to do it.

If the users like what they see when we demonstrate it, we leave it with them, as we did with collaborative planning. I was out in San Diego in August 1993, and we had a program called Target that ARPA had developed for collaborative planning. We planned a whole scenario for Korea in 30 minutes using video and this collaborative planning. The CINC liked it, and the Joint Task Force (JTF) commander liked it. We now have that software program and are trying to integrate it into the Global Command and Control System as a module so that anybody who wants to can use it.

Student: Okay, sir, I've got it. Thank you. Let me ask you this. I'm sensing that the capabilities that you're offering are so sophisticated that they're outpacing the ability of a prospective JTF commander to keep up with them. Here's what I mean. Currently when we select JTFs, it's either done ad hoc—you know, guys from varied headquarters—or we build on a service component, a three-star guy that the CINC has. Let's say that Admiral Macke and CINCPAC turn to Lieutenant Jones, 1st MAC, and say, "I want you to do this." Well, unless he's been working with sophisticated things such as you offer in these systems, I don't see how he can use them to their full robustness.

Edmonds: That's a good point. Let me tell you two things. First of all, this technology we're talking about right here is mostly point-and-shoot/click kind of stuff. That's the first thing. The second thing is that, based on those kinds of concerns, we're filling it ourselves right now: we're putting teams on the ground for training, and we're going to keep teams on the ground training for a year, and supporting it for a year. The problem hasn't been the fact that it's sophisticated; the problem has been that those three-stars you talked about have a tendency to want to stay with the things they know and they've done. A lot of that is outmoded, outdated, and not very useful, and most important, it's not interoperable with anything else around. As a matter of fact, General Shelton was happy with that MSE he had out at Haiti, but I was not very happy about it at all because the only way he could make that phone call was for me to run a communication line all the way back to Fort Bragg, back to an

* Lieutenant General Shelton, 18th Airborne Corps Commander.

Army post, to talk to an MSE kind of thing because it's an Army-unique capability.

Having said that, every day we're trying to find ways to make that a transparent problem so that we don't have to go back to Fort Bragg to do that, because it's cheaper to go from a satellite right into Haiti, or from the *Mount Whitney* right into Haiti, rather than go back by way of Fort Bragg. Until such time as the users get this kind of capability in their hands, they're going to keep using those old capabilities. They will keep being limited by the information they have available to them, because this system, for instance, can give them intelligence, it can give them operations, it can give them weather, it can give them all the things that they have right now that take them four, five, or six systems to get.

What else are we doing? We also just created a five-day course out at George Mason University for orientation, to try to get two- and three- and one-star potential Joint Task Force commanders to understand these kinds of things. We're also sending kids from Keesler Air Force Base (the Air Force training center) around to military bases and posts teaching this kind of stuff. We're also putting a course on DISA and on GCCS onto our DISA network on the Internet so people can pull it up and go through step-by-step instructions.

The real case here, where you make a good point, is that nobody expected us to be successful. They thought it would be 5 or 10 years and a $500 million or $2 billion program. WWMCCS cost $350 million when we started doing this. Today I'm maintaining the old WWMCCS and implementing this program with $107 million because the technology is cheaper, we're doing client/server instead of mainframe, we're point-and-shoot, we took all the software like Windows, like when you use Microsoft, to do this. The only thing is that people kind of say, "I don't get to see all of this. You guys must be doing something funny in the back room." The fact is, that's the beauty of this technology. If you don't bog yourself down with some old legacy stuff that won't allow you to move when the technology changes, you're okay. So what we've done is try to change the mindset. This technology will change every 18 to 24 months, in my opinion, and if you buy into anything that will not allow you to refresh yourself, you're buying yourself a real low stall. That's why the ARPA/DISA office for technology keeps this stuff fresh, so it won't get old.

Student: Sir, I tell you, this is great. I'm listening to your last sentence so I won't monopolize the entire discussion as I often do. I want you to know that next month I've been invited to the Pentagon to brief a concept I have called "Joint Task Force Headquarters 21." It's a structure of Joint Task Force headquarters for the 21st century that involves each CINC getting a standing JTF. One of the main reasons, among others, for these standing JTFs is so that when increasingly sophisticated technologies and systems such as this come out, you have guys who are dedicated to warfighting at the joint level, and they can continually be refreshed on this kind of capability. They'll know what all the services can do in terms of warfighting and be able to integrate these things synergistically, et cetera. So I just want to let you know that this is great.

Edmonds: That's what I want to do.

Oettinger: Stay with it for just one second because I want to pursue your question.

Student: She looks like she's going to throw her coffee on me if I say anything.

Oettinger: That's all right. I'm saying it—you're not, you see—so you're off the hook. She can throw her coffee at me.

I thought you might be going in a somewhat different direction because the question you raised struck me as rather similar to some of the questions that Admiral Owens put before us when he was here.* We say this is all well and good. It is remarkably here today, as opposed to being always on the drawing boards. But the question he was raising was that, assuming not only this but some of the other things are now reality, then the whole concept of

* See Admiral Owens' presentation in this volume.

what you do on the battlefield may be profoundly altered. You may recall I took issue with him on the notion that total battlefield awareness might not be real dominance, et cetera, but if you accept the notion that, absent the usual countermeasures and so on, something radically different might happen, you really have to think it through. The fact that it may get degraded by countermeasures is a whole other matter. But I think that you're seeing the beginning of something which may require fundamental rethinking of what it is you do.

Student: I strongly agree.

Oettinger: We want to tie that back to Admiral Owens' remarks and the discussion we had at that time, because you're sticking a little close to what happened today and tomorrow, and General Edmonds was trying to get us to talk about down the road. This may be a whole new ballgame.

Edmonds: As a matter of fact, I modeled Admiral Owens' 2010 notion. I spent two hours with him and Dr. Deutch and I've gone back to model what happens with all this stuff in 2010, because that's what he wanted to ask about. I told them I can deal with 2010, but the thing I've got to get us up to is right now, because right now I don't have a lot of force structure who understand this stuff. They're wedded to the old ways, and the reason for it is because they didn't think about doing anything and we've got something for the warrior right now. Also, we've got CINC and service participation.

But the main thing we did is, we had no grand design (figure 12). I would not let anybody design a program for me and tell me "Here are the milestones, and here's what you're going to produce at the end of those milestones." I would not. The way I got around that is that Admiral Jeremiah* took me up to meet Deutch and Perry and I said, "Okay, this is what we're going to do for C4I for the Warrior. We have a quick-fix phase, a mid-term phase, and an objective phase, and we are in the mid-term. The objective I can deal with any way you want me to deal with it. Just tell me what year to pick. But no great design."

- **Get capability to the warrior now!**
- **CINC and service participation key**
- **No "grand design"**
- **Modular design**

Figure 12
A Tough Challenge

Up until now, until they put the IG (Inspector General) on me, I had refused to go to a MAISRC (Major Automated Information System Review Council) or DAB (Defense Acquisition Board). I'm implemented now. So now the IG said, "Okay, you can take this off because you haven't done it like everybody else. We're going to let you go ahead and do this because it's good and the warfighters want it, but I want you to go ahead and give me a life-cycle program after October." I said, "Okay, I'll do anything, because I'm going to be finished with this by October." So I agreed to that. But "no grand design" is important, because I have changed more than once in terms of the direction in which we took this program. When I left the Joint Staff, the only thing the Chairman said was, "You can leave the Joint Staff right now and go to DISA if you take GCCS with you, because I don't want this design to change."

Modular design is critical. If you have a module for fire support in the Army that is the best module for fire support, and everybody will need a fire support module, we'll take that module and plug it in, and we'll kind of fix it up so the Navy and the Air Force will like it, and then that will become the fire support module. And we'll change next year!

Student: This is great stuff!

Oettinger: Leave it right there, because again I want to underscore that "no grand design" for those of you who are not

* Admiral David E. Jeremiah, Vice Chairman, Joint Chiefs of Staff, 1990–1994.

cognoscenti. Look at the record of the last and preceding years. The orthodox view is that the only way you do this is by having grand designs to implement, et cetera, and of course if you look at Tom Quinn's comments,* there is a 10-year procurement cycle, so by the time your grand design has been accomplished, it is obsolete 10 times over. The notion that in order to deal with current technology change, external world condition change, et cetera, you have to do what is being described here, and to see that advocated not by some wild-eyed speculator, but by a three-star general who is responsible for getting something done, is a radical change that has happened over the last year or two. So you're witnesses here to a radical change in the way things get done. Is that a fair statement?

Edmonds: That's a fair statement.

Student: But sir, what's the downside of that? There's got to be a bummer in there.

Edmonds: Its downside is that if you change horses in the middle of the stream, you'd be dead. If I hadn't taken this program from the Joint Staff to DISA, this program would probably be in trouble. As a matter of fact, the very people who want you to do the grand design will take the power structure and put it against you. We had to fight for money. We had to fight for how much testing we were going to do, how much documentation we were going to do, how much *this* we're going to do, how much *that* we're going to do. We're going to fail, or the customer will be happy. Customer participation has been very important to us. The only way we survived is that the CINCs and the warfighters said, "We need this!"

Oettinger: Correct me if I'm embroidering nonsense, but aside from personality and politics and so forth, one of the other things he said earlier is that the technology is getting cheaper. So if you're in a period of declining budgets, and you have this mission and continuity that he just described, and you're able to take old programs that cost *yea*, and you do it 10 times better at less cost, you have a chance. If you tried to do this in a period of rising technology costs, then, everything else being equal—including his three stars and his approach to things—it would probably be dead.

Edmonds: Yes, because you could not sustain it. You'd go back every six months and you'd have a program overrun, and then the program leaders would just kill you. I can get almost as much power on a minicomputer now as we could get on the old mainframes that cost you a lot of money to maintain, and every time I turn one off, I save money. That's what Jerry Tuttle did. Jerry Tuttle turned off WWMCCS computers in the Navy, took the money, and put communication on the ships. He did it without telling a lot of people what he was doing, and by the time they woke up, it was done. Then they asked, "What has he done?" I remember the message he sent out: "If you're in the Navy and you want to do some WWMCCS processing, the only place you're going to get that done is at Norfolk." There were no other Navy WWMCCS terminals or mainframes. Every time he turned one off, he saved millions of dollars. He took the millions of dollars and he bought SHF (super-high-frequency) satellite capability for the ships. Now watch them do it!

Student: General, how portable or easy is it actually to get this to the warrior? Can you put this on an airplane? Can you put it in a tank?

Edmonds: We can put it on an old NEACP (National Emergency Airborne Command Post) now called NAOC (National Airborne Operations Center). The objective of this program is to run on any platform you can get. We've tried to become platform-insensitive. Right now we know of two that run it without any modifi-

---

* Thomas P. Quinn, "Acquiring C^3 Systems for the Department of Defense: Process and Problems," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1994*. Program on Information Resources Policy, Harvard University, Cambridge, MA, January 1995.

cations: HP and Sun. DEC has invested their own money to run it. The reason why it's important is because if you go into the system and you already have a Unisys environment, I don't want you to go buy a bunch of hardware. So we're going to make this software available to people to go in and find out how to run it on a laptop.

Student: A follow-up question then: If I can run this on my laptop, or if I can run this in the back of my aircraft or whatever, what's the medium that gets the information back and forth that makes it a live system? How are you transmitting it?

Edmonds: We use all of them. The DISN, that Defense Information Systems Network, includes commercial satellite, military satellite, fiber, air-ground UHF, air-ground SHF. The Secretary of Defense uses SHF on the NAOC.

Student: So, a final question then: What I would do is, for example (because I know airplanes), I take this laptop, I plug it into one of the radios on my aircraft, and then use that?

Edmonds: As a matter of fact, it's what you would put in your bus, because I want you to have a monitor bus in your airplane in the future. You do data processing and fiber on the airplane so you can put a bit through quick, and you can do bus communication packets, rather than a stream that had to be very wide. You want to do data compression and, as a matter of fact, we're doing that right now.

Student: Which is also easier to protect as information.

Edmonds: Exactly!

Oettinger: Again, if I may underscore, you're riding a trend that will last (as far as we can tell) for the rest of your working life. Because that stuff is getting not only faster and cheaper and better, but also smaller, the old shibboleths about "There is no room in the platform and we cannot tolerate the weight" are gone, because you can always take out old heavier crap and replace it with smaller, cheaper equipment that will fit in the space. As a matter of fact, you save weight and space, so that there's an extraordinary confluence here of technology and organizational opportunity and budget, all of which you have to look at in order to understand what's going on.

Edmonds: That's correct. We have some airplanes at Andrews Air Force Base, 137-Bs, old models, that we use to haul people around. They're going to go out of inventory in less than five years, so we can't do any modifications on them. So the Secretary of Defense asked me to look at fixing some of those airplanes' communications, because they're really bad. But I got the Secretary of the Air Force to agree to one thing: let me take out the old equipment, and just put a plug on there. So now when they use those airplanes, they come with two suitcases. They plug in the computer. They plug in the comm—the radio, modern stuff. And it went up, just like that, overnight.

I'll tell you something else we're doing. We put INMARSAT on some of those same airplanes. We put airphones on the same airplane. We have a problem with securing the airphones, like the ones you have on the regular commercial airliners. If you could secure them right now, I'd have them on all those airplanes. So I have NSA working on securing those airphones, because those technologies are available to us. The throughput is fantastic, and the quality is good. I got on the airplane and flew around up to New Jersey to check the quality I could get for the Secretary of Defense. This stuff is not very expensive. You're talking hundreds of dollars and tens of dollars rather than millions of dollars. On new airplanes, when we get those, we're going to harness packed modules, so you can take modules and plug them in or out—bus. That's the way we're going to go in the future. Technology costs, sizes and weights are helping us because it's happening so rapidly. So that's why you don't have to worry about what you're doing today, because tomorrow I'll give you something better.

Student: General, if the vision of the information infrastructure that you suggested will allow users at all levels to use the same information, and have access to information horizontally and vertically, does that not lead to a new vulnerability in the sense that now everybody's sharing the same information? And not only that, it's reaching everybody, so if you're sharing the wrong information, then the damage done could be very great.

Edmonds: The sharing of information is a good point. The notion is that you're going to have selective availability of data to people who need to know certain things. We've always had that as a criterion. For instance, if I'm in intelligence and I need to know some intelligence information, that's one thing. If I'm in logistics, I probably don't need to know much about SIGINT (signals intelligence), for example. So you need access codes and those kinds of things.

Remember the definition I had about fused information? I've always said, and I believe this in my heart, that I would not want to make a decision based on one bit of information unless I was in a critical situation. I want two, three, or four sources of information to fuse in order to come to a conclusion. That's kind of how we make decisions. Except in the past, we've taken days and weeks to come to those conclusions, and now you can do it right now. I get some human intelligence, I get some signals intelligence, communications intelligence, so you know this as of seven o'clock this morning. So if you know what the weather is now over Baghdad, I can tell you what it was at seven o'clock this morning, or I can give you a feed at two o'clock. A lot of information can be perishable.

Let me tell you another thing, too. The other notion that we kind of thought about in this whole process here is that we expected that the warrior will want to have a certain amount of information already captured, as the basis of what he's going to do. For example, in a war plan, you have target sets. We have them all the time. You have offset points, aim points for dropping your bombs, and that kind of stuff. Sometimes you also want to make sure that you get intelligence to update the information that you already have rather than get a whole new dump. So on my way to my target area, I can get a new bit of information that the target I was about to hit is now gone, or they rolled in some surface-to-air missiles, and now the threat is no longer at *this* level, it's at *that* level. So I either have to go higher or go around or do something else. I want to get information pull more than push. I never felt that the warrior wanted this information just for the sake of having it.

Oettinger: I sensed in his question some overtone also of trust, and it seems to me that over lunch you said a few things about the people involved, which might be worth reiterating here in this context.

Edmonds: That's a very good point. Remember I mentioned a program called Target, and I said it was collaborative planning. There are two good things about collaborative planning. One, it has a video link and an audio link out to the warfighter. You can see them and you can hear them. A very critical thing about warfighting, and a very critical about planning and this whole thing, is trust and knowing people. There are several people who went to Harvard with me, they went to Capstone—my one-star course—with me, and they went to war college with me: both allies as well as other services. General Sheehan is the ACOM commander, the CINC. He and I were Capstone classmates. The Vice Commandant of the Marine Corps and I were classmates. A lot of my classmates have four stars already, but you know, that's not all bad. It's really good. I live on a street with 35 generals and four admirals, and we get to know each other.

One of my war college classmates was Prince Khalid, the guy who was the coalition co-commander with General Schwarzkopf out in Desert Storm. Khalid's brother is ambassador to the United States from Saudi Arabia. I know them very well. So if we're getting ready to do secure voice with them, we provide them with secure telephones, and we provide secure conver-

sation with them. It's the same thing with the French and with the British.

There's a certain amount of credibility that comes with knowing whom you're talking to. In most of our secure voice, especially the good stuff that we have now, we have voice recognition. I know I'm talking to you. I know you're telling me good information. That's the best credibility I know. A platoon sergeant or a tank guy who is driving a tank hears his company commander say, "Okay, troops, this is the order of the day." Everybody can hear him, and you can authenticate to get good information. So this mutual trust in the system is kind of like the question you asked about training Joint Task Force commanders, training Joint Task Forces before you go, so that you know how you're going to fight when you go and it becomes routine for you. That's all a very important part of this in terms of keeping your confidence up.

Student: In fact, I believe that training and all that would help to increase the trust and so on, but actually the problem could be the other way: that you become so dependent on something when you don't even know what's going on. It's just this electronic medium that's invisible, and you just plug it in whenever you want information. You become kind of dependent on it. I remember Admiral Owens also made a remark about taking out some of the so-called obsolete old systems like SRS and T-1, and said he was the one who was very much for it: just take it out and don't worry about it. So you are going to have less access to systems which you have more direct control over, and you're just going to depend on your intelligence inputs from this big infrastructure.

Edmonds: There's nothing better than human intelligence, if you trust it. In the Special Operations Forces, I would put my trust in five guys from Special Operations Command on the ground in our enemy's capital rather than 25 orbits around the globe. If I have those 25 orbits, I'll take them and validate what they've already told me, but five guys whom I drop behind the lines, who then will go and tell me where the power plant is for the target, are worth their weight in gold. And so, I don't ever think one bit of information is what you want to go on.

The other thing is: we can give you not only electronic information, we can also show you pictures. What Admiral Owens can tell you, and I can tell you here, is that we can put in your cockpit the real picture of the target so you can look at it and say, "Yes, that's it!" We've got target parts and navigation parts in our LANTIRN (low-altitude navigation targeting infrared for night). We can put a building right over there on the pod, on the sensor, and pick that building out with everything on it, and know that's the right building to hit. With some of our tools, we can go right through that third window from the right over there. That's pretty good information. That's credible information.

Information is the real difference here between winning and losing the next war. Al Campen* will tell you that in the last war we had our eyes and ears on. The enemy's were off. We turned his off. That's the difference. If I can put a missile through that third window from the right from three miles out, and I can launch my rocket and leave before they even know it's inbound, that's information, that's power. I have all the confidence in the world in that. I've seen it done in practice; I've seen it done in real. So that's the kind of confidence you're looking for, really. Believe it or not, 10 years ago I would have said I would have problems with technology, but today, technology is that good. As a matter of fact, it's almost too good.

Student: You keep talking about the user in this whole loop. How does a system like this affect the sources? I'll ask it three ways. Does it increase or decrease the number of sources that are required? Does it change the proximity of the source to the actual event? And how does that affect those sources? Do you need more? Do you need less?

---

* Alan D. Campen, *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War.* Fairfax, VA: AFCEA International Press, 1992.

Edmonds: All of the above. Let me give you an example. On the screen of the Global Command and Control System, I can click on an icon called Intel. Based on what I want to know, I can click on the next thing, and it will tell me what I want to know. Do I want imagery? Do I want SIGINT? Do I want to deal with InteLink? InteLink is a thing they put in about a year ago. It goes around to all the databases, the CIA, FBI, DIA, NSA, and in those databases they've got old historical data that shows you pictures, information about Guatemala or whatever, and you can study it. You don't have to print it, you can just study it. That's one bit of information. Oh, by the way, you want some HUMINT? You can get some HUMINT that's been debriefed and put into the system. You want to get communications intelligence as of right now? The thing about it is that you always have a picture of the battlespace. You know that the P-3 might be up. You know that the E-3 might be up. You know the JSTARS (Joint Surveillance Target Attack Radar System) might be up. If you want that datalink information, real time, live, right then, you can pull it. Whatever you want! It's the user, it's the customer, it's the commander, it's the operator. What do I need to make my decision? What do I need to do my job right now? If it's some data from last week, I'll use that. If it's data I need today, right this moment, I can pull that.

That's what we're trying to give them: that kind of fusion, that kind of information pull. Admiral Owens talked about those UAVs (unmanned aerial vehicles), downlink and everything, and they're going to give you more options, more information to pull. What are they looking at? They're looking over there, 200 miles out. They're looking 20 miles out. I'm on a ship, an Aegis cruiser, and I've got all kinds of stuff to do the same kind of things. I look at this and I say, "I have my mission for today also."

Student: What kind of retrieval message do you use? If you want people to pull information, you have to give them a lot of leverage, because somebody should be able to say, "I want anything about Guatemala. I'm not really sure what I need, so give me ... "

Edmonds: In this system, we have a structure, and our focus is the Joint Task Force commander, the person on the scene running the show, as the center of our universe. You have to start at the center of the universe. It's easy then to let anybody above him have a terminal or a screen to look at it.

Another very key thing is that we made a conscious decision to make this system be Secret and below, not Top Secret, not codeword, not compartmented information where you have to know everything about everybody to get the information. So this is not something that's going to give you some great big advantage. If you aren't cleared for that information and you happen to see something, you don't have to say, "Hey, this is something I need to do something with." The fact that it's going to be encrypted means we don't worry about people who don't have a need to know having access to the information, because they're going to have clearances.

So let's say you're in logistics or supply. We don't really care if you find out what the weather is over the target area. So we're not going to limit your access to the weather. There might be some things we might limit access to, simply by code, by the need to know. But we really want the warriors be able to pull the information out of this system, whatever they need. I don't think the warrior in this case will necessarily always be the guy who is pulling the trigger. If you're the logistician providing bombs and bullets for this mission, you're one of my warriors. You've got to get those bombs on the flightline. You've got to requisition some more. If you need some pilots or some infantrymen, and they're back in Fort Hood, Texas, or some tank drivers, you've got to go into the personnel system and order some personnel, so you need to have access. This program has a security plan, a security architecture, and we've structured it around those kinds of things. But the center of our universe is the Joint Task Force commander.

Oettinger: I'll let you move on, but I think the thrust of the question in part was that you've got these floodgates, you've got all this stuff for the guy, but how does he know what to pull and how to interpret it? I guess the short answer is that tools are being developed, people have to learn, and today's three-year-old will do it better than anybody in this room because although you're all young, you are already too old to master most of these systems, and for three-year-olds who sign on and teach themselves, it will be different.

Student: My two-and-a-half-year-old does that right now on the computer—logging on, changing programs, and all that.

Student: Jumping on that point then, Professor Oettinger, when we talk about operators—the junior enlisted company-grade officers—are the skills that are being required of these systems in sync with (a) the quality of recruit that we're trying to get, and (b) the missions and skills that the Training and Doctrine Command is putting out in training these people? Or are we hoping that there is also a leap in the educational system so that our youngsters are getting to learn this?

Edmonds: The youngsters are not the problem. The problems are the oldsters. The youngsters can do it in the speed of light. As a matter of fact, the people who do most of the demonstrations are two-stripers and three-stripers. We showed this to Dr. Kaminski* over at my place. We had somebody who had been on it for about four hours doing a demonstration for us. I used to do computers years ago, but I didn't do any computer operations kind of stuff like e-mail until about three years ago. I just refused to do it. I don't want to be one of those.

One of the volumes in our technical architecture is a man-machine interface volume. But the funny thing about it is that after you start doing a little bit, one click leads you to the next click. You almost can't miss the right clicks. I keep trying what I think might be hard, but if I miss the first click, usually the second one is okay. That's why I made them do click-and-shoot rather than all this "Open Apple 3, 4, 5, 6, 7, 8, 9, 10 ... ," because I didn't want to learn all those numbers and alphabets.

So basically we got a mouse. You click and you say, "Okay, Mission, *click*," or "Fighters, *click*." It's a picture! Most of them are pictures. There are not an awful lot of words. We click and shoot. If you want to see ships, click on the ship. If you want to find the *Eisenhower* and how many airplanes you've got on there, click on weapons systems, airplanes. Click on munitions. You've got a bullet sign there. We really have done this thing that way because all those guys will have read that there will be an E-7, E-8 somewhere in the system who will say, "I can't get through this thing. It's absolutely too complex to give you the information you want, boss." I don't want that E-7, E-8 doing the work. I want that boss to be clicking, and when he clicks on that screen to see it, everybody says, "We've got 18 airplanes, *click*. We've got 24 bombs. We can do 18 missions plus 6," or whatever you want to do. You can do planning.

You know what's good about it? As Tony said, we've done so well with this enterprise integration now that as we take down those bombs and put them on those airplanes to do the mission, we're taking out my supplies at the same time, and it's also creating the requisition to order some more. That's happening in this system. So the commanders then say, "Okay, let's have our staff meeting. You go back and debrief. We're clicking and shooting."

To tell you the truth, the old guys my age and the rest of them are trying for this stuff not to be good. They keep looking for the panacea. "Oh, this couldn't be this easy. This couldn't be this simple. This couldn't be this cheap. You can't do this for one-third the price and give us all this. There's a catch somewhere, Al, where is it? What are you going to tell me tomorrow? Are you going to tell me you need $2 billion tomorrow? You can't install this stuff, can you?"

Let me tell you something else. As we were installing it, I had guys say, "You

* Dr. Paul G. Kaminski, Under Secretary of Defense for Acquisition and Technology.

have no business installing this stuff." I said, "Why?" "The services should install it." I'll go back to the question we had a few minutes ago. The services don't have the talent to install it because they don't know what it is we're trying to do. They've been fighting the problem. They're waiting for five years to go by to get on board. So we want to make sure it's successful. We're installing it, but we're also training, and we're paying for it, and we're teaching, so it will be successful. They don't have another choice.

So it's breaking culture. It's breaking down the paradigms that everybody has been used to doing. "Don't worry about it! It won't come on my watch. Ten years from now, I'll be retired, and you guys will still be trying to do that. You'll need five starts and the program will take your money from you in the fourth year because the program manager can't explain what happened to the money three years ago." I have a program like that right now. They gave us $150 million three years ago to do something this year. All the money's gone and they can't figure out why we didn't do anything. I said, "I wish I knew."

When I showed it to the Chairman, he said, "This is fantastic!" I said, "What do you mean?" He was out in Washington State, working with technology doctrine kind of stuff, and it ended up it couldn't produce anything because they always brought the killers in to tell what they needed. By the time they got it all defined, one killer left and a new killer came in. One was artillery, and one was armor, and they had different needs. If you look at the history of our acquisition system in this government, very rarely has it produced anything other than those big ticket items where you go out and tell somebody to build a lot of airplanes for us, and we would modify them a lot. But things like this they never produced, never.

Now let me move on so I can answer some more of your questions. As a bonus, we only reengineered what was appropriate (figure 13). We checked the all the users involved. I paid for the users' TDY (temporary duty). I paid for their travel to come up and sit down with us. "Play with this! Tell

- **Reengineer only where appropriate**
- **User involvement at every step**
- **Select "best of breed"**
- **Iterative prototyping with maximum reality checking**

Figure 13

A Novel Approach

us what's good about it. Tell us what you don't like about it. Give us feedback." Then I told them, "We'll select the best of the breed." That's how I picked the Navy system. We also told them we were going to do a lot of iterative prototyping, a maximum reality check. Do you know what a maximum reality check is? "You tell me, customer, what you want." So later on, they looked at the system and they said, "You're making a lot of changes." Yes, because they're telling us what they want. We got them involved in reengineering my program.

I'd just like to show this picture (figure 14), but this is what I want to tell you. Remember I told you about the standards, architectures, common operating environment, buying commercial off-the-shelf products, and not a lot of R&D? That's a killer, any time, any place!

Let me get to the next program. I told you about the transmission part—the Defense Information Systems Network. These are the goals (figure 15). (1) Satisfy the Joint Staff validated warfighting requirements. (2) Get the terminals from the FTS-2000 (that's a federal telecommunications service that offers information technology). GSA sells telephone services to us. We take advantage of them when we can, and we provide our own service. HAWS is the Hawaii area wideband system. We buy our own service if we have to. We're now doing the DOD/GSA integrated approach to try to get economies of scale and provide the best transmission media available. That's what that really means. That's the transmission, the pipes, the circuits, satellite links, comm lines, DMS—Defense Messaging. These are things I exploded a few minutes ago.

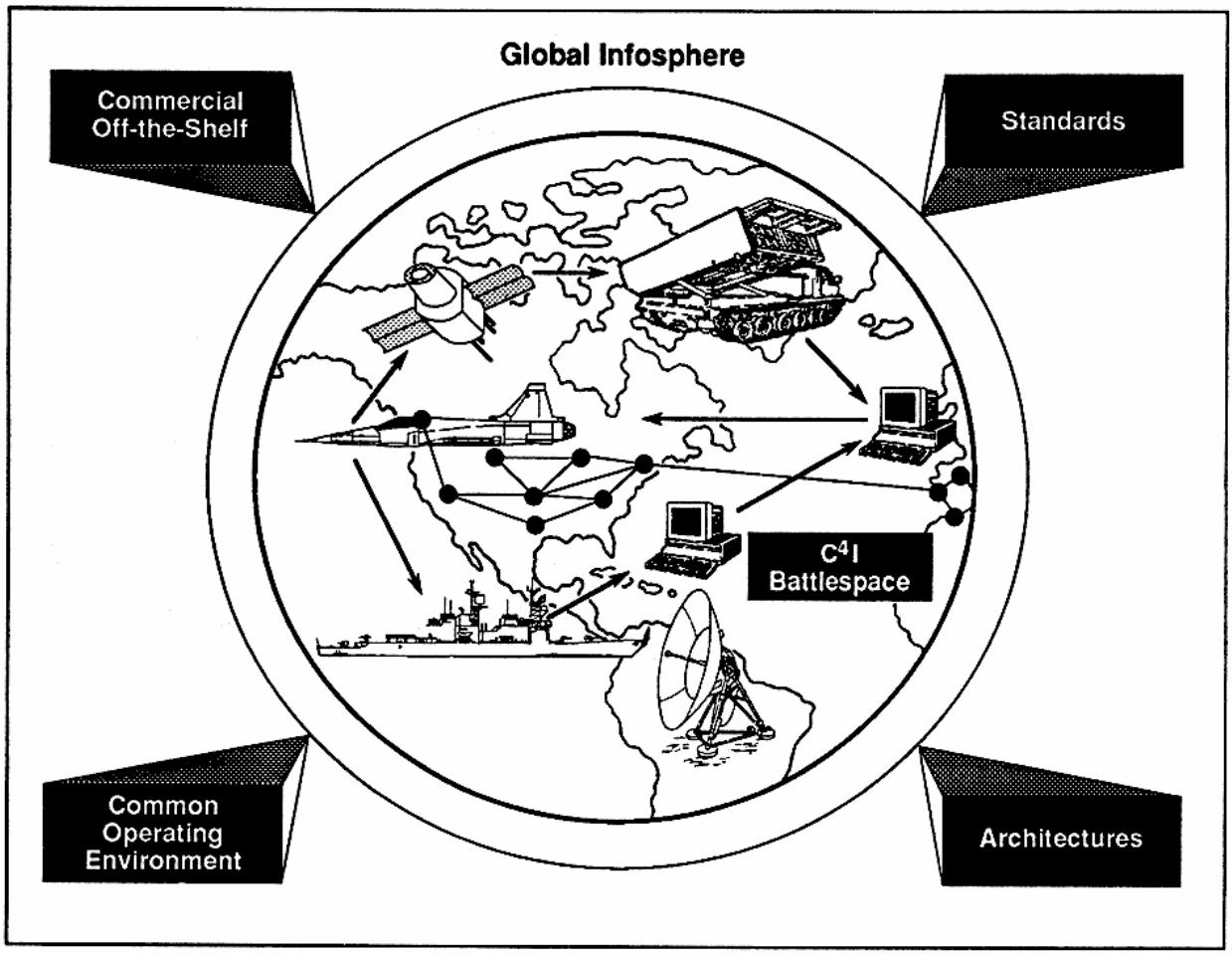


Figure 14

GCCS: An Integrated Global Environment

Defense Messaging—this is a very important slide right here (figure 16). This is the transmission part. Remember when I talked about all the "II"s in the slide with the global grid? The Defense Messaging infrastructure will allow us to message from the home station, to in transit, to deployed. This is almost a total other briefing. Our architecture will allow you to use your home computer on the airplane in transit, or in the foxhole, to move your messages anywhere, any time, any place. That's our objective for this program.

Now, where are we on this theme? What's the tasking (figure 17)? You notice that every time I put a slide up, I tell you to support the deployed warfighter. I phased out AUTODIN—remember I told you about the old system, the old analog data message system? Other features are reduced cost, and look at this one: standardized e-mail. Around the Department of Defense, we've got so many different kinds of e-mail I can't even count them. It's like a dog breakfast!

Student: General, would your idea then be that pretty much every DOD member would have an e-mail address for communication, from the lowest to the highest?

Edmonds: Yes, everybody.

Student: No reason not to, right?

Edmonds: Everybody, everybody. Everybody will have a messaging capability.

Let me show you an example (figure 18). We talk about technology and how things have changed in cost. The current

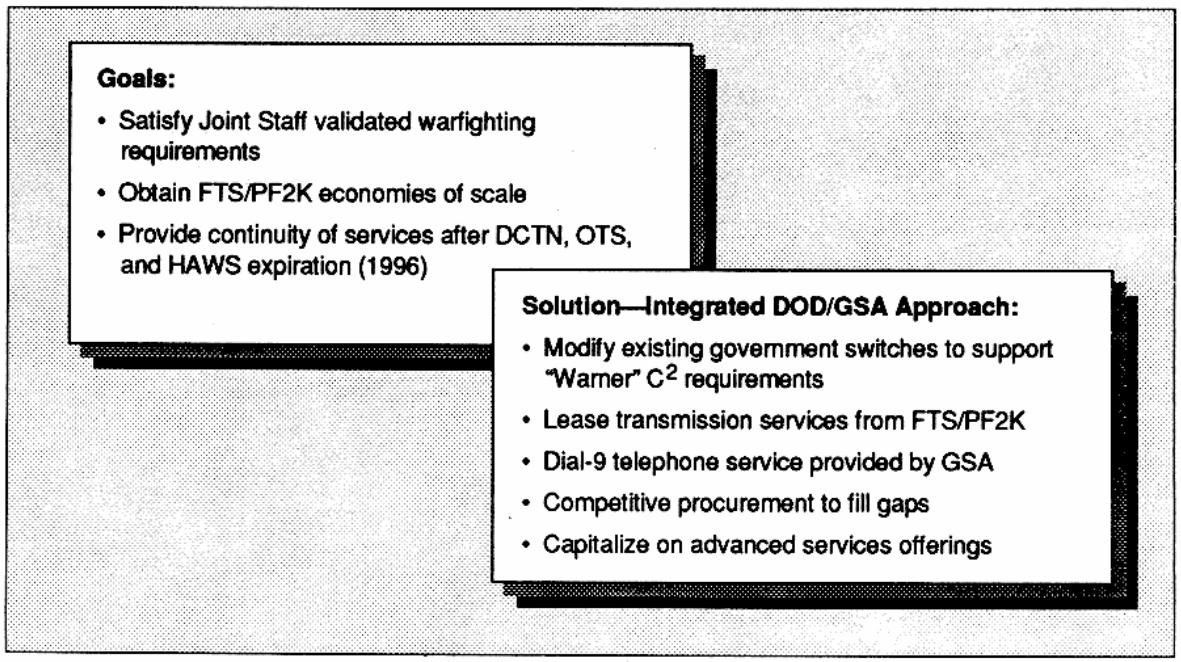


Figure 15

Where We Are: NII/GII Drives Change in Course

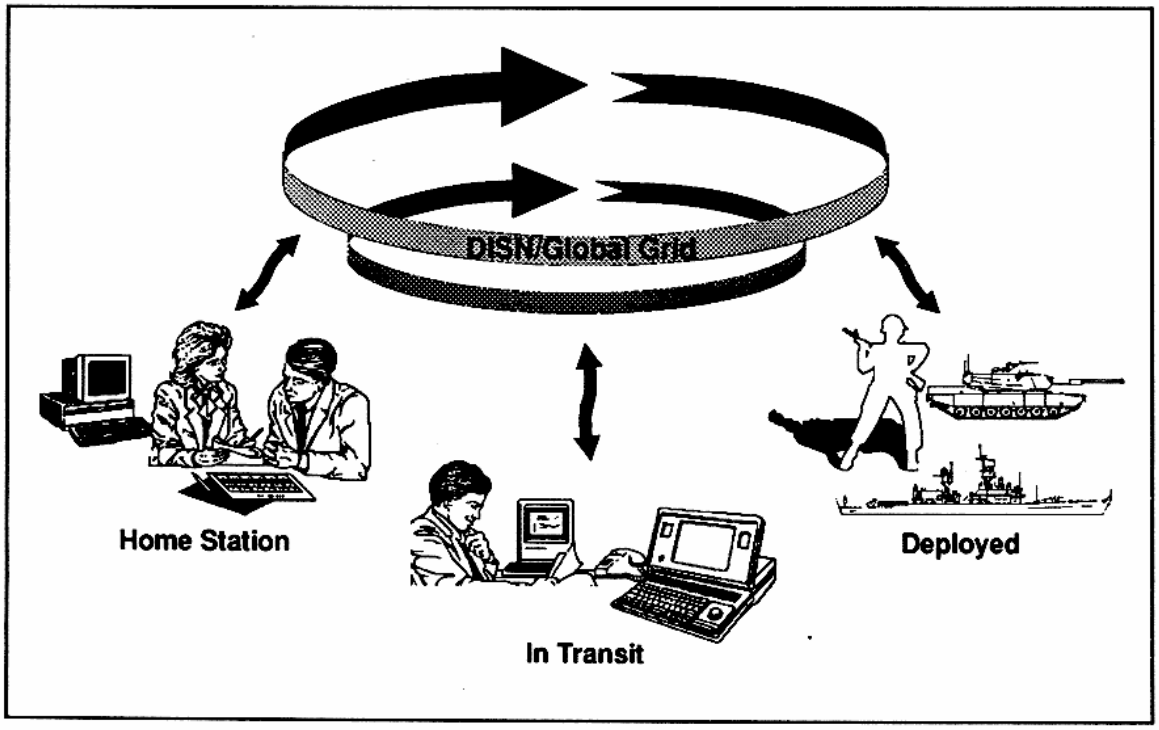


Figure 16

DMS

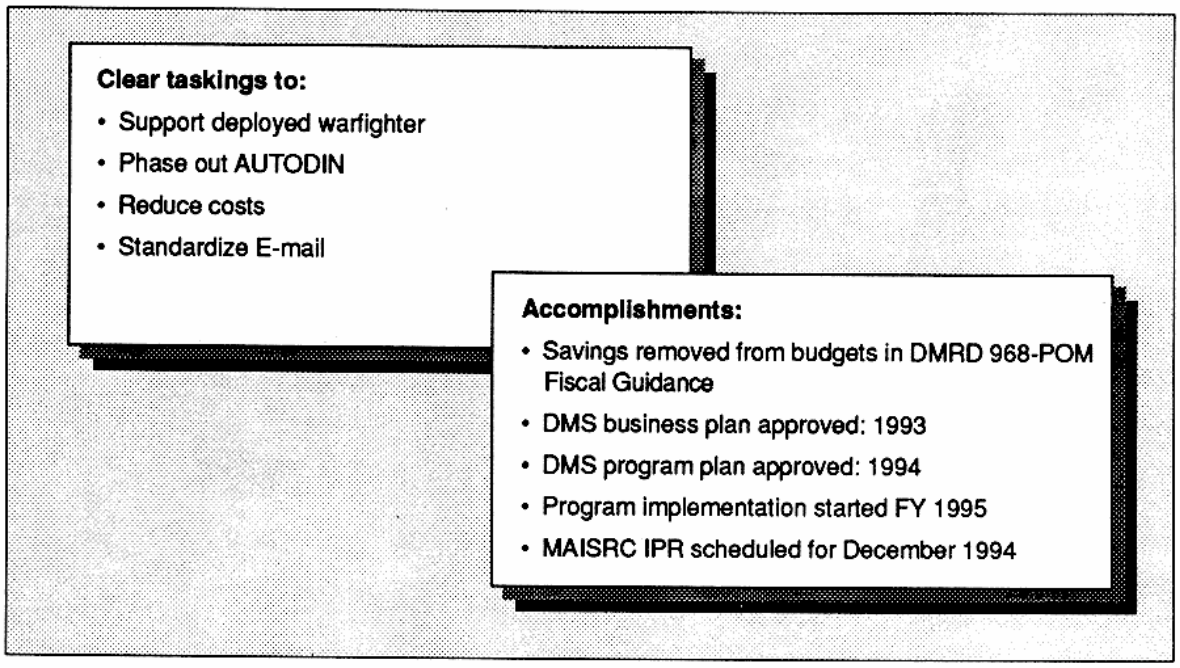


Figure 17

Where We Are: Program Documentation Approved

AUTODIN system that doesn't do e-mail, that just does those messages you get through your office in the morning on the board, would cost us over $500 million for the next five years or so if we were to stay the course and continue AUTODIN. This system is older than anybody in this room, probably, besides me and a couple of others. When I was a second lieutenant, I used to do testing acceptance for this system. It was a mainframe. It used to be a hard-core computer. Look at the prices for this Defense Message System I'm talking about. This is the full program. It replaces all of the AUTODIN functions, and it gives us standard e-mail as a bonus. That's what it does. Look at it! Tremendous!

Oettinger: I just want to add, this is continuing—the cost drop and the capability increase from what's in the laboratory now are good for another decade at least, just on the basis of the elaborate new science stuff.

Edmonds: It just keeps going down. So you'd be crazy to get locked into anything for a long time.

Now this is the new stuff. This is the good stuff. It's going to be on the test: information warfare/INFOSEC. I use INFOSEC because when you say "information warfare," everybody wants to own it. We do the defensive part in DISA, and this is my charter for doing that (figure 19). I'm not looking for policy. I have a mission statement—DOD Directive 3600.1. It tells me, "... as central manager for the DII [remember that old thing I liked, the DII? It's ours] ... we are to assure that DII contains adequate protection against attack." That's all the charter I need. That's another thing I've been watching. When they give you the charter, you take it, and everything that's not nailed down, you take that too.

Oettinger: Can I ask you an impertinent question? Are you able to do whatever the hell you want without NSA's blessing? Or do you have to do a little foot, toe, and arm wrestling?

Edmonds: NSA and I have a joint office where we do work together to put this together. NSA can't do things in space. I'm

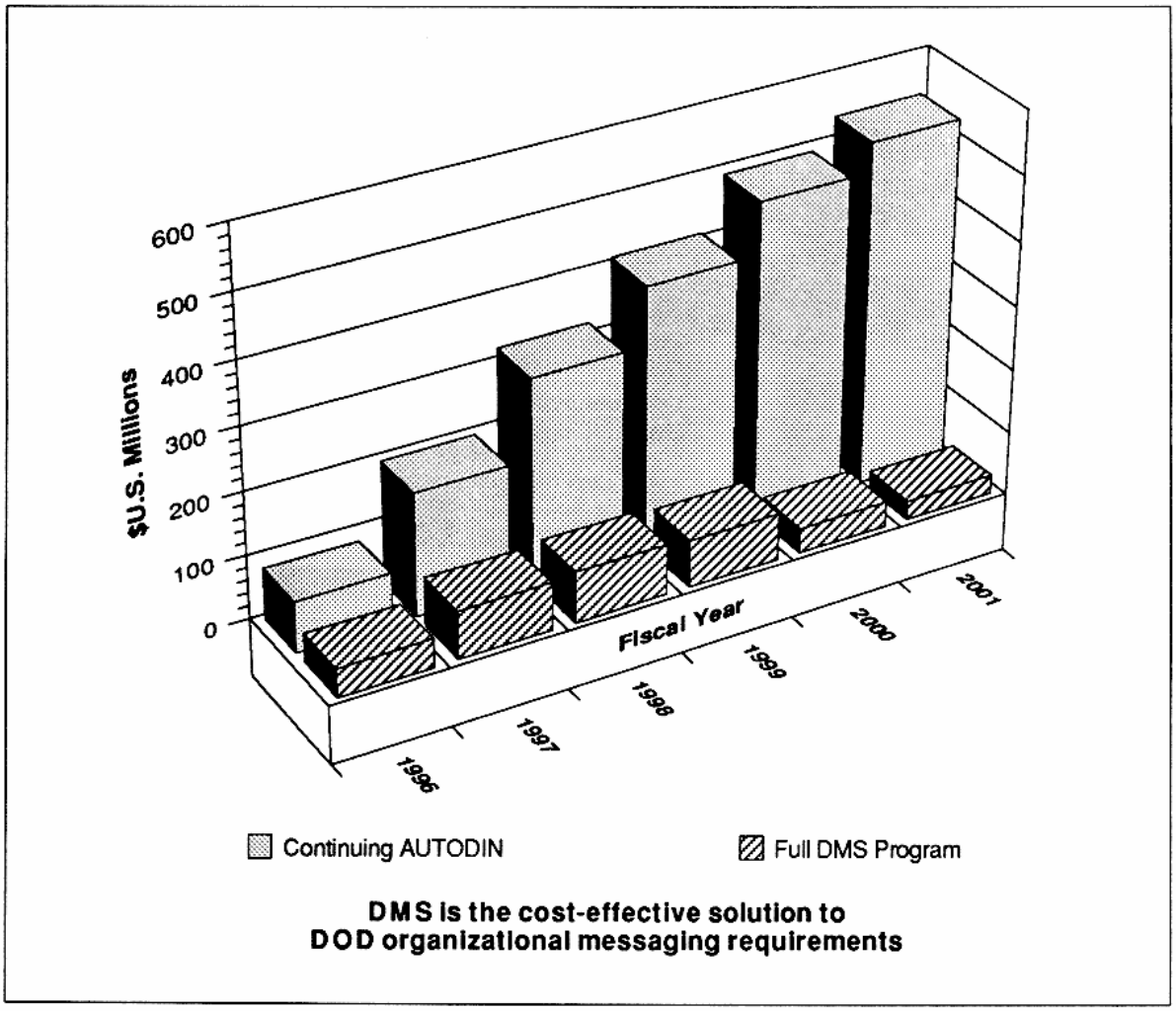


Figure 18
DMS vs. AUTODIN

> **"...As central manager for the DII, shall ensure the DII contains adequate protection against attack."**
>
> DOD D 3600.1

Figure 19
DISA INFOSEC Mission

the production guy. They help me with products and with technical assistance.

Oettinger: A very interesting relationship.

Edmonds: Very interesting. We work together. We've got to make sure that our system can withstand an attack (figure 20). I put a few other terms up here because everybody talks about hackers all the time. We all know about jamming. People don't think about deception, masquerading, or malicious code, but we talked over lunch about malicious code. If you streamline the government and I'm a computer programmer, and you give me my pink slip and in two weeks my job is gone, I might say, "Hmm, how can I pay myself two weeks from now? I'll put some malicious code in

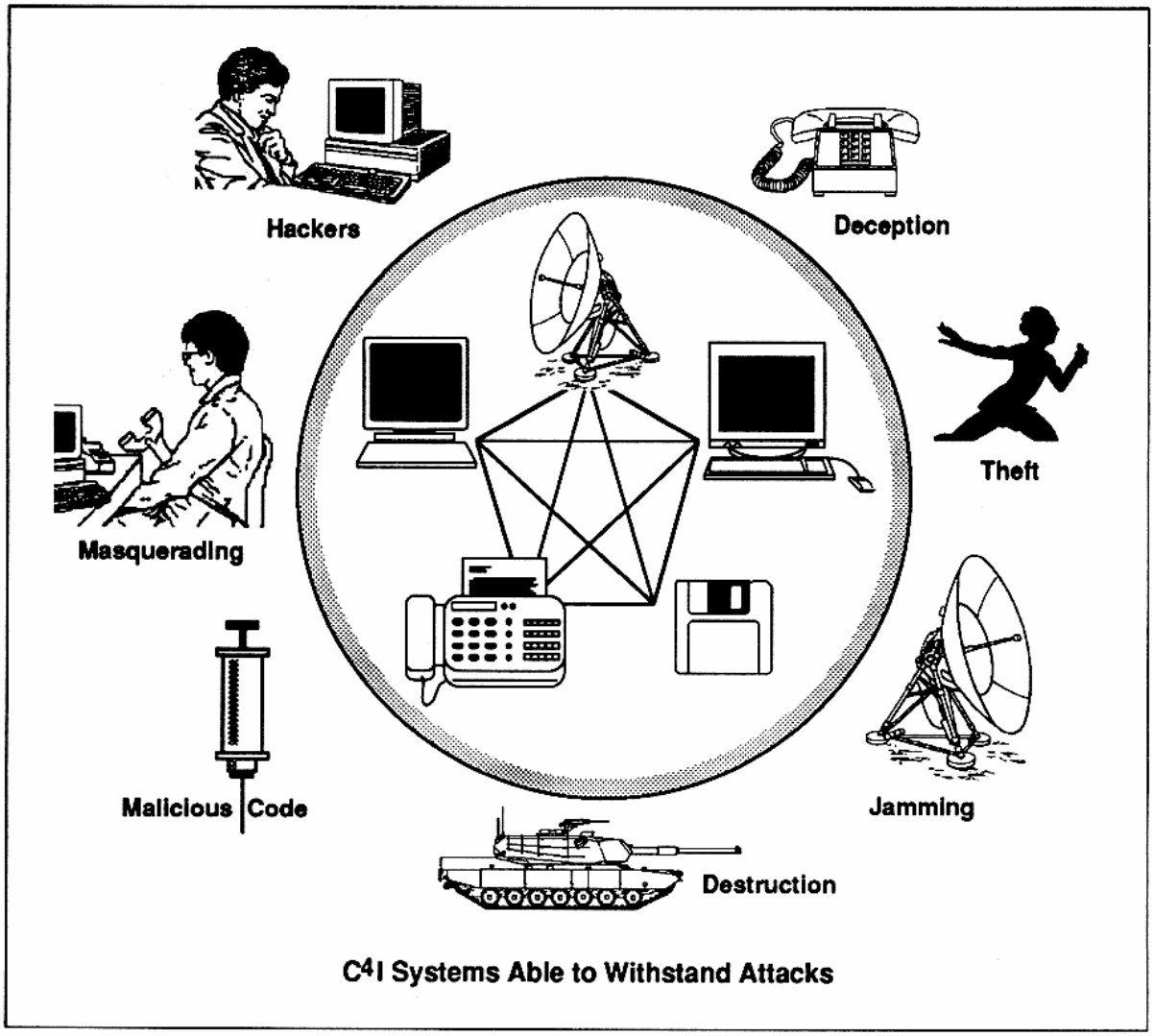


Figure 20
Protection

there to get me a couple of checks." It's a very big risk. Or he'll just take the system down, take the whole company down. How about taking the whole telephone switch down? Why not take the whole system down?

Masquerading. Suppose I'm an Army man, and suppose you have troops, and I call and tell you, "Take those troops and move them to Harvard Square and have them down there by 1500!" and about 1505 I come in low level with an F-16 and drop a bomb on them because I'm masquerading as somebody you trusted (this is back to the trust point again), and you can't detect that it's not the right person. It's a very important thing to protect ourselves against.

Oettinger: But before you go on, I want to underscore again something that General Edmonds went over extremely lightly—so lightly he didn't even mention it. But it goes back to the earlier discussion about doctrine change and what happens when you have brand new things. What he slipped over on you was that he's in charge of protecting both computers and communications, and he called it INFOSEC. If you look through all of the past years of this seminar, there were years and years of

battle over who owned communications and who owned computers and so forth. Not until that little doctrinal ownership, et cetera, thing could be solved could this kind of thing happen. It's happened, you see, to the point where you don't even feel obliged to mention it. When there is a sea change like that, radical things happen. All that has changed is an idea, but it's taken years and years to change that idea. Now it leaves no traces. It's awfully important for you guys to grasp, because he didn't say it explicitly: that you couldn't do a bloody thing until that idea changed.

Edmonds: Exactly, and that's what you see in this circle in the middle of the chart. That's your computers, your comm lines, floppies, telephones, satellites, all of it. Take that, that's part of the charter. Protect that infrastructure.

Let me just tell you why it's a change (figure 21). First of all, there's a lot of information flowing. Everybody likes information. I found out that if people know

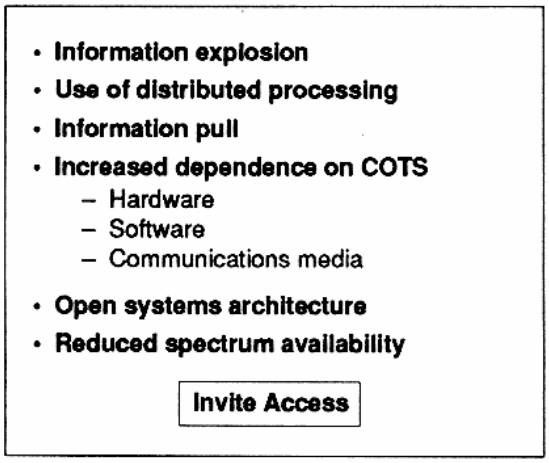


Figure 21

Changes in C4I

one thing, they like to pass on this kind of information. You think I'm kidding you? Just let somebody go out and fall on the step downstairs where you walk and you say, "Guess what! Dr. Oettinger fell down the step down there." You don't say anything about the fact that the poor man broke his head, busted his head open, he's bleeding, unless you feel really bad because you tripped him. You just like to pass on information. So a lot of information is passive, and you take that and multiply it by everything you know.

The Pentagon says that information is power. When I was a major down there, I knew a lot of guys, like this young man, who used to walk around with a little briefcase with locks on it. That meant he had a secret in there and you couldn't get the secret. He went inside the building to the Chief of Staff of the Air Force, the Secretary of the Air Force, and then he looked around in his other pocket and got the key, and came around and unlocked it for the boss to read it. He didn't leave it with him, either. The boss read it, and he got it back from him, and he put on it, "Have seen." He put it back in the briefcase, locked it back up, and came back out the door. Those guys always had a little hump in their back there. That's where they had all the information. That was power! And all those guys who didn't have a briefcase would say, "Wow, I wish I had his job! He's got access. You know, he gets into all the main men's offices."

When I got to have these three stars here, folks started to bring their little folders to me. There isn't anything in them! Everything is in *USA Today*! They're trying to get me to read stuff I don't want to read. They say, "So you want to read the intelligence books?" "Oh, yeah, bring it on in here." I open it up, and I look at it, and it talks about some stuff I read two weeks ago in one of the trade journals. But the report that finally got printed finally showed up in their folder, and they've got Top Secret on it and all the funny words down at the bottom and stuff, and it's got a lock on it. Those cats will not leave the front of your door until you read it. They won't leave it with you, either. They take it away. So this kind of exposure makes you very vulnerable.

Distributed processing means there's processing all over the place. There's information pull. We're using off-the-shelf products, and a lot of our software, a lot of our things, are being done overseas using open systems. Everybody is smart in this stuff. The United States is not the only

country in the world that's smart. So we don't have a corner on the market.

Reduced spectrum availability—frequencies—result because when you take away the frequencies and sell them to the commercial people who build stuff around them, you just narrowed the frequency you can use for military kinds of things, and it makes a smaller target. So we are inviting access with some of these changes going on.

Who are the people that are playing in this thing? I'm going to talk about some more of this in a minute. Everybody you can think of are players (figure 22). In the middle is DISA, and it shows you data, network, systems, spectrum, all of that. NSA is helping me with vulnerability analysis. I have a National Communications System (NCS) hat that I wear. In time of war, the Communications Act of 1934 says that the Department of Defense is responsible for *all* of the telecommunications network in this country. Under that hat, the Secretary of Defense delegated that responsibility to me. So right now, for instance, out of Oklahoma City, I have a team helping coordinate communications for a lot of activity out there because the cellular frequencies are jammed. We want to make sure that MCI, Sprint, and AT&T can get stuff through. That is our national security emergency preparedness. We accept the priorities of people to use it. We decide whether the Red Cross or the Department of Agriculture or somebody else gets the comm line. There's one line. That's one of my hats. I have a center on the second floor of my building, which was activated yesterday and has been going 24 hours a day, that's working this part of it with FEMA and with Justice, with DOD, and everybody. My guy on the scene out at Oklahoma is a GSA guy. He's our regional, national communications systems guy, because all the federal government are members of the NCS.

I told you about the joint program office we have with ARPA. It's no longer DARPA; it's ARPA.

Of course, there's industry, because industry has a big role to play if you're talking about commercial products. So these are the players.

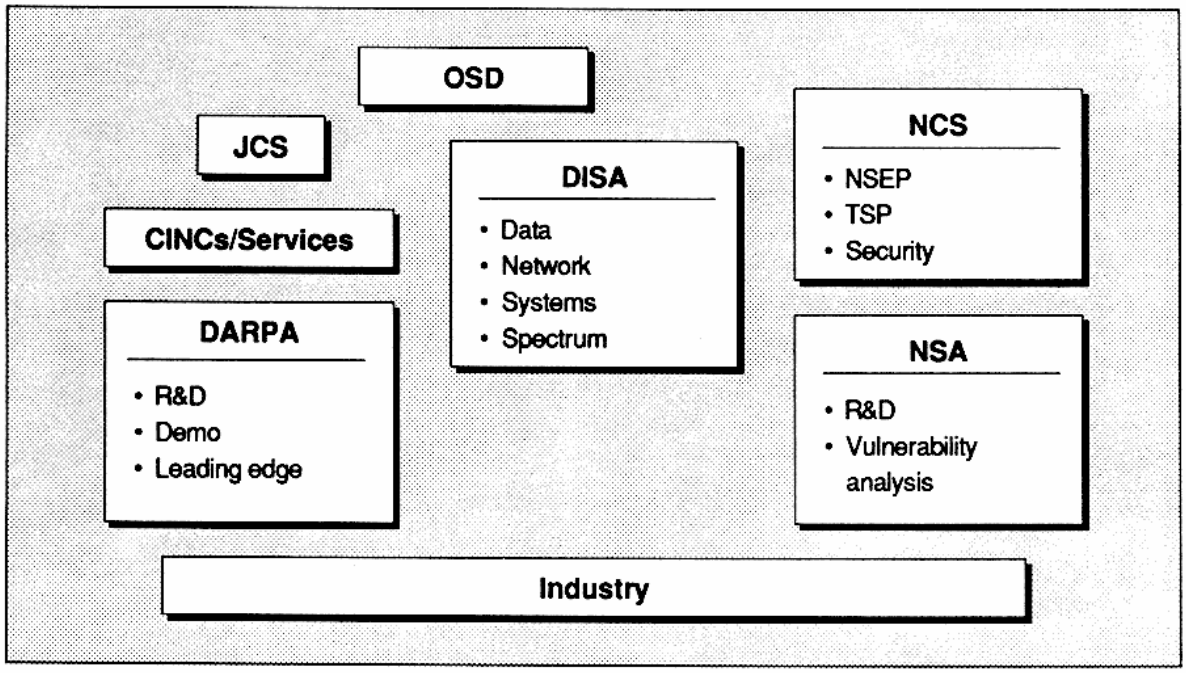


Figure 22
INFOSEC Partners

Now let me tell you some other things that will blow your mind here (figure 23). I told you earlier that I'm going to address the infrastructure—not just system or network protection, but the whole infrastructure. We're going to protect the information commensurate with the intended use. There are some things that need not be protected, so we won't protect them. If there's a thing that needs to be protected with crypto, we'll encrypt it. There are no two ways about it. For the other things you should have privacy. So we're going to build these programs around what needs to happen with current things, not what people want.

If you think this is not very important, let me give you some data (figure 24). I have a team called the ASSIST—Automated Systems Security Incident Support Team. The slide says 17 hours, but I made the duty day 24 hours. We always have a duty officer available. We have responded to more than 7,000 calls for assistance so far. We've done these kind of countermeasures alerts. We tell folks what to look out for if they have a system. We also give a technical analysis if they ask. As a matter of fact, I've been out to CINCTRANS and CINCSTRAT to kind of help everybody with their system. We also do vulnerability analysis, so if you have a system and want to know how vulnerable you are, just ask and we'll help you. We also train you to do it yourselves.

But let me tell you some things that we found out from those folks we evaluated, and this will really blow your mind. We figured that 88 percent of the DOD unclassified systems we've seen are easy to

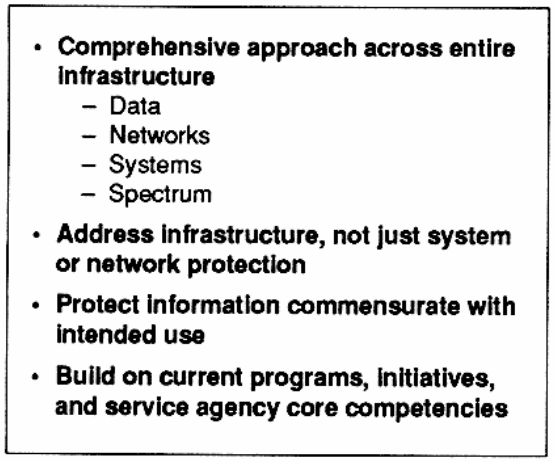


Figure 23

INFOSEC: Strategy and Approach

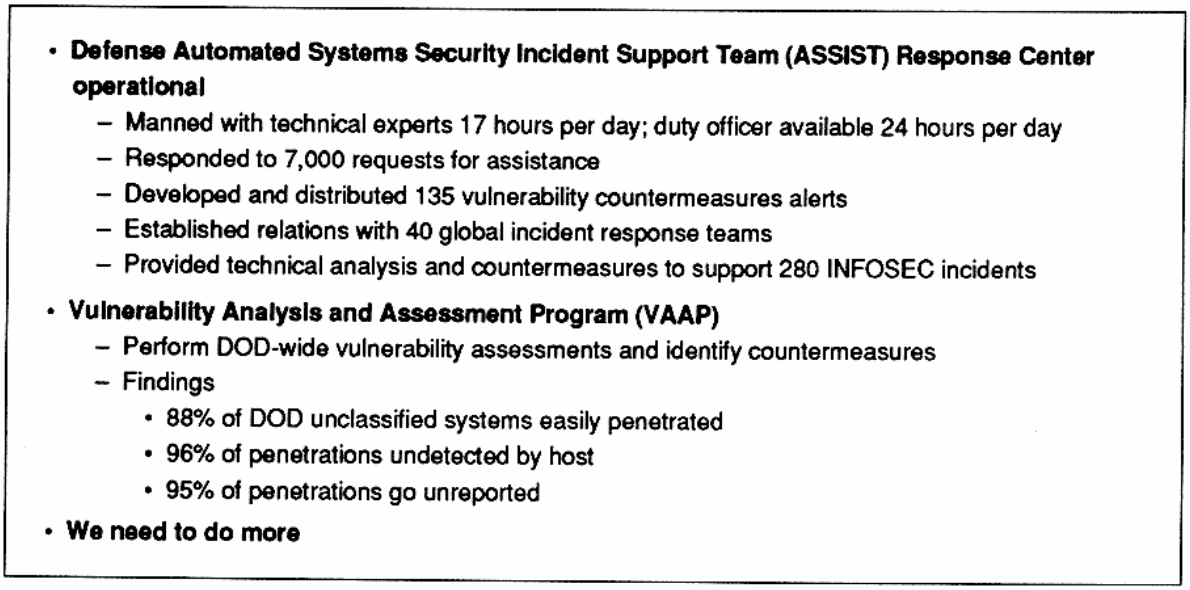


Figure 24

INFOSEC

penetrate. With 96 percent of those we penetrate, they don't even know we've done it, and the few who know you've done it are so embarrassed they don't tell anybody. They won't admit it. That's a fact.

Oettinger: Just think about it, guys, because that's true of your own computers as well.

Edmonds: Exactly! There is probably not a single computer in this room that we can't get into. Not only can we get into it, we can also change the data. We can manipulate it. We can dilute it. We can turn it off. We can break it. This is not a whole lot of sophistication here, these are things that you can get on the market.

Student: Do you just do this for DOD, or do you offer this to other people? If, for example, I work for Cambridge Hospital over here, or something like that, can I pick up the phone and call you guys and say I want a vulnerability analysis?

Edmonds: No. We do DOD, primarily because people are afraid of DOD, and they don't want to get involved with that stuff. Now in my other hat, my NCS hat, what I'm trying to do is to get the other federal government agencies on board—the Commerce Department, Treasury—and we're working that very smartly. But it's hard to get the rest of the commercial entities involved.

Oettinger: That has been an intractable problem so far.

Edmonds: That's the government versus civilians, and there's not a whole lot of trust.

I'm now going to talk about what the C4 future holds. This is going to be kind of hard to read, but I want to leave these with you because they are very important.

In my mind, the thing that is going to get us through and help us save money and continue to reduce costs is for us come up with some data standardization (figure 25). There are some de facto standard things out there, like the ones who set the de facto standard for manufacturing computers in this country. Whether you like it or not, Microsoft Windows set a lot of standards in this country. Everybody has gone out and

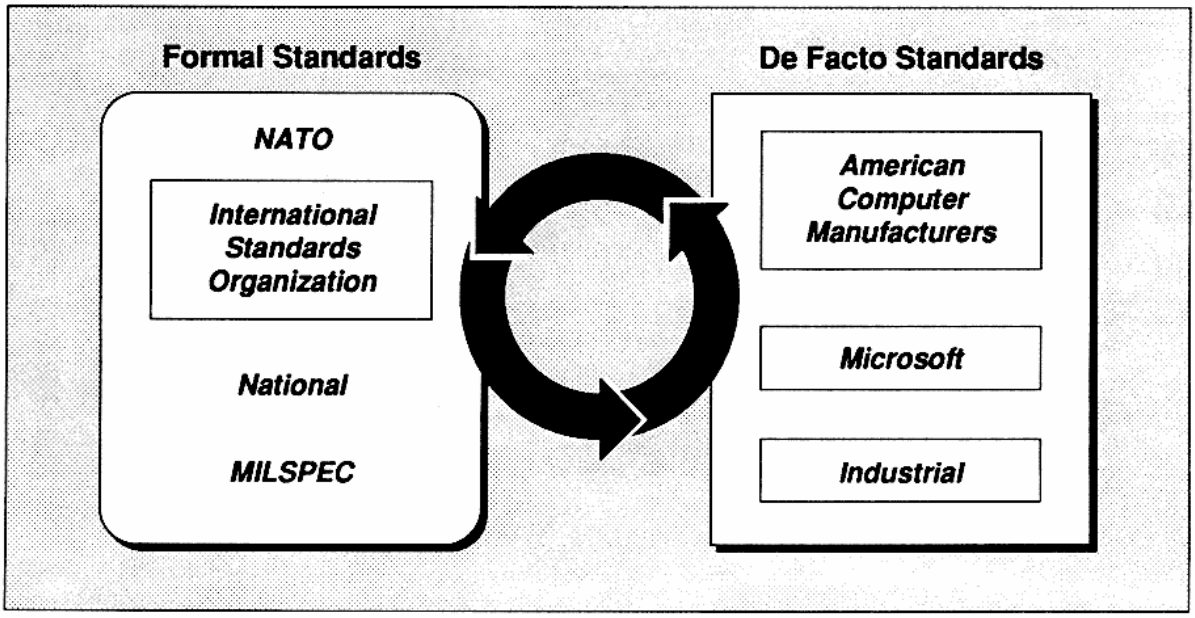


Figure 25

Data Standardization

tried to find a Windows motif to kind of build to, so it looked like the same thing, and of course there's the industrial sector.

Allies and international standards are very important. We're trying to do less MILSPEC, and almost no national standards. Only a few things are MILSPECed, because a few things are military owned. Almost everything we're trying to do is commercial, and we hope that industry will accept it and it will become national and international. We're very successful in this area. We're very successful with NATO and with the Pacific Rim nations because we're using the same information and the same approach with NATO and our Pacific allies. We have formal entities to work these kinds of things.

Data standardization is very important. Right now we have 2,379 standard data elements in the Department of Defense, and we're going to have 9,000 by September. We're going to issue those as our core data elements and make them available to industry as well as government. So if you're going to build a DOD software system, or develop one from scratch, you use those 9,000 data elements as your core and you'll be okay.

The other thing that goes with that is what I call our Technical Architecture Framework for Information Management (figure 26). Standard data elements is one piece. The TAFIM, what you call the technical architecture, is another piece. Let me

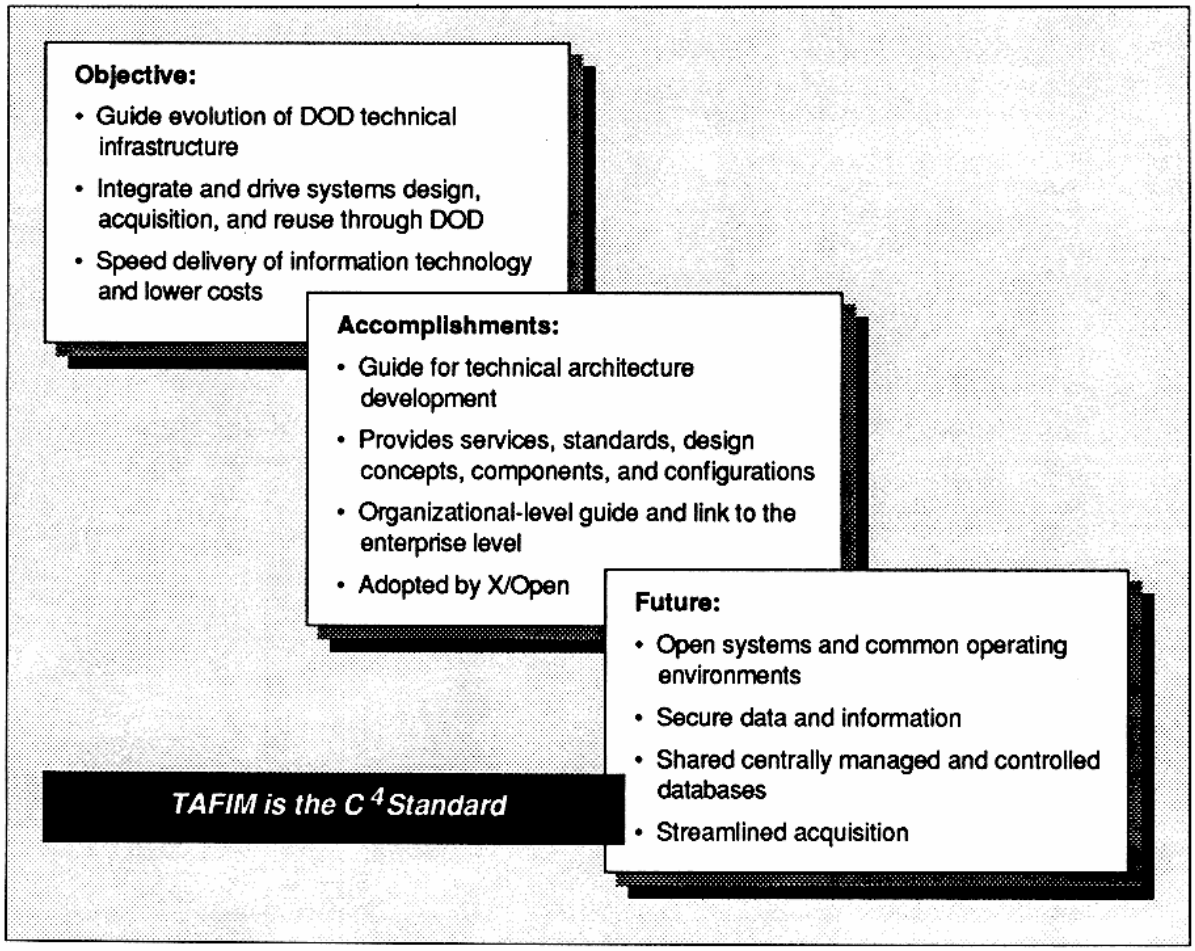


Figure 26

Technical Architecture Framework for Information Management (TAFIM)

tell you what's in there so you can see it. Here are the eight volumes (figure 27). I didn't like them at first because there were too many of them. But I've opened up a few of them and they're like books. Once you open them up and read them, you like them a lot better, especially the thick ones. There's a Technical Reference Model, Architecture Concept and Design, Standards-Based Architectural Planning, Support Plan, DOD Goal Security Architecture, and look at this one, Human-Computer Interface Guide ... absolutely wonderful. Now industry is thinking about adopting these as commercial, because they think that by doing that they're not in sync with DOD. So they built our standard data elements, used these guides right here, and there's just one little piece left. Guess what that piece is! The common operating environment of GCCS. And there you go (figure 28).

Now whatever you think about it, it's not important at this moment. What I'm going to tell you is that we recognize the big external environments (that's the comm links), whatever they are, satellites or whatever. There are a lot of databases out there, external things—open systems conformant, operating systems services. These are common platform services, program services, and user interface services, like X-Windows. Look at it! And then support applications: business processing, baseline, standard applications, and we allow the services—Army, Navy, Air Force, Marine Corps, and the SOF guys—to have some of those unique kinds of things because we know there are some service-unique kinds

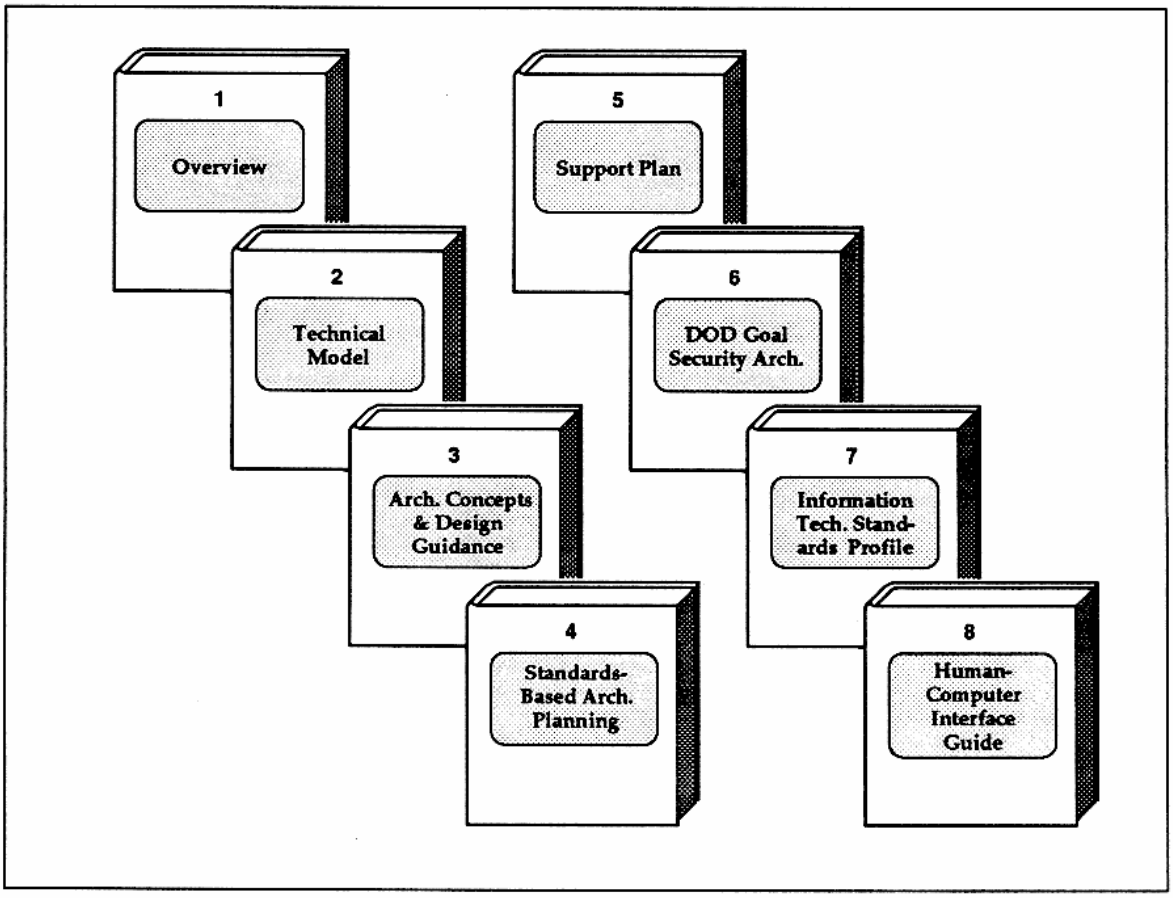


Figure 27
TAFIM Volumes

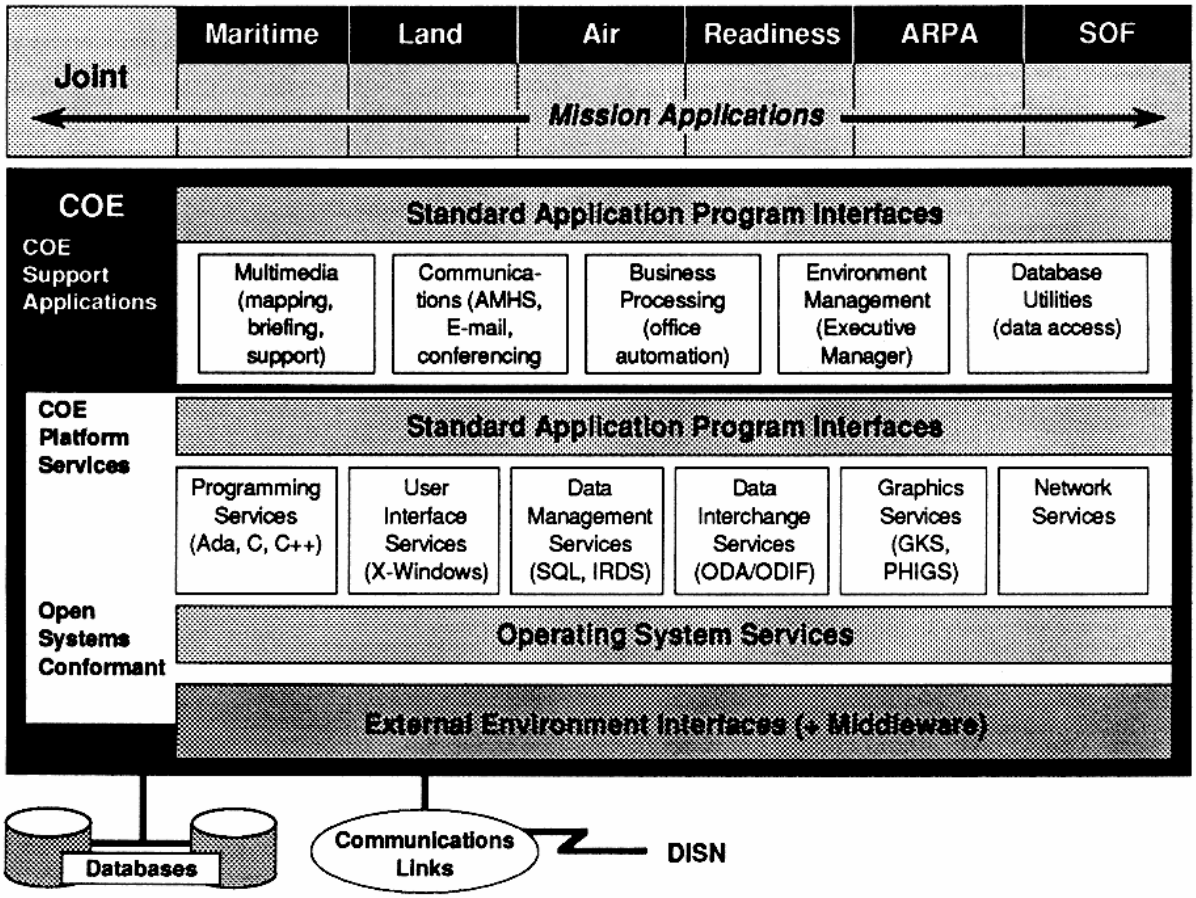


Figure 28

GCCS COE

of things. It's foolish to say that there aren't. That includes the readiness stuff like status reports. We have mission applications that are joint, and some uniques. So if you build to this common operating environment with the TAFIM, with the standard data elements, you have a pretty good chance of being interoperable.

Let me give you another look at that, and once more this is not an eye test (figure 29). I just want to show you that the GCCS baseline involves architectural guidelines and the common operating environment. We've already fielded 13 of 19 modules. The services are going to nominate those other six modules to us. These things came from the services. We didn't develop these separately. We took a good chunk of what was already in the Navy system. The other services nominated pieces of the GCCS. We took them and worked to integrate them with the rest of the environment.

Software tools. We got some online access libraries, some integration tools, some runtime tools to execute your libraries, and that's how we do it. That's the model.

Now let me tell you what we're doing in standardization. You say, "Why is this data standardization stuff important?" I like this slide (figure 30). The reason I like this slide is because I can talk to the fighter pilot with this slide. I can talk to anybody with this slide. Day, month, year. How many times have you filled in an application blank and you don't know if they want the day first or the month first, but you know the year is usually last? That's the only thing you can tell. I can tell you that I can find multiple systems with the date as many ways as you can take six or three and multiply them or divide them, add them or

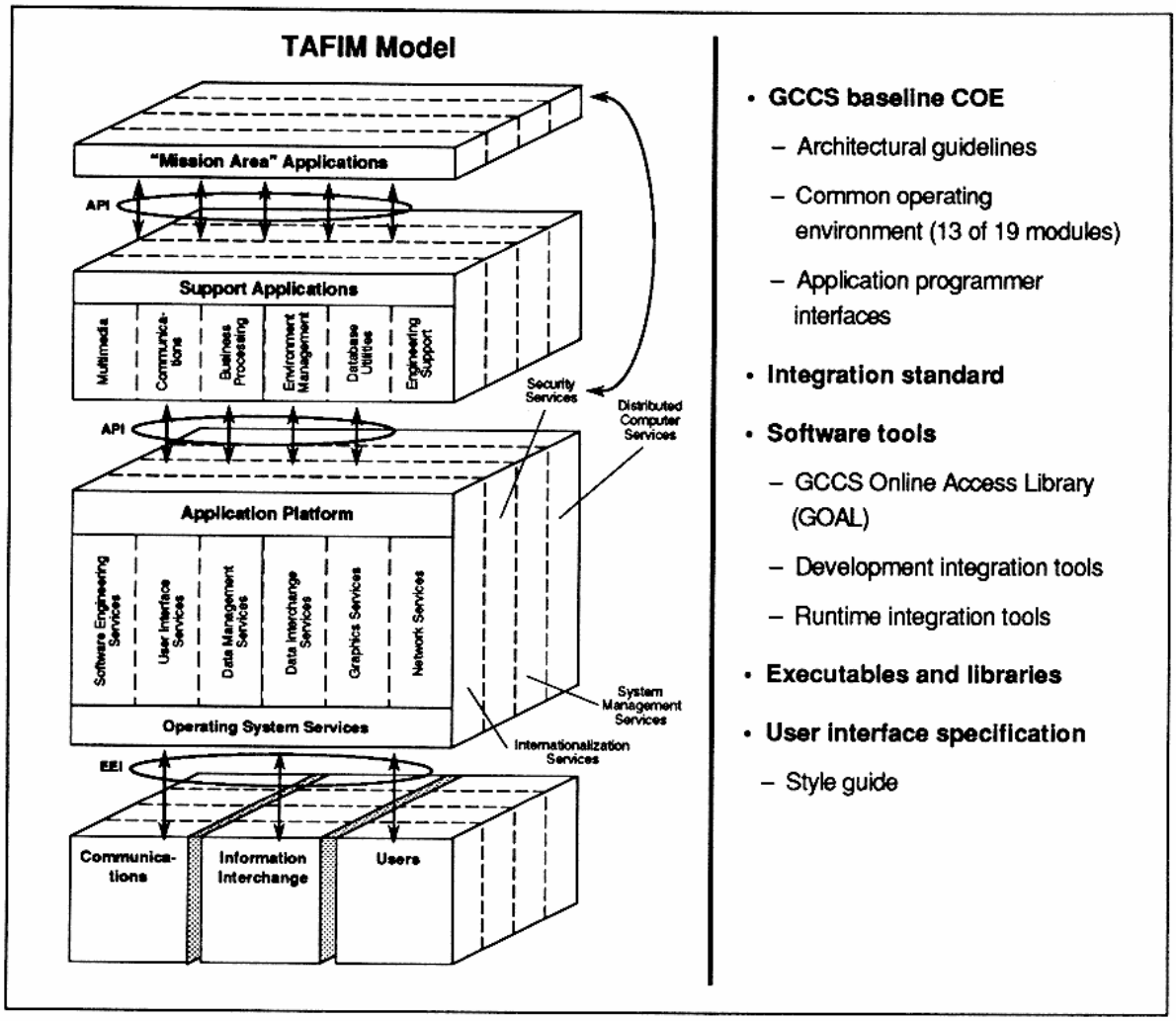


Figure 29

The TAFIM and GCCS COE: The Keys to Success

subtract them. The whole notion is to find a single way of saying what the date is, or what a tank is, or what a bed is. A bed is not the same as a bedpan. Believe it or not, we argue over those kinds of things because the person in charge of beds may not be in charge of bedpans, and the one who's in charge of the beds says, "You don't do anything with this data element, because that's mine." The bed folks might be the supply sergeants. The bedpan people might be the nurses. Tell me which one is which! But that's why standard data elements are important, so that we all build to them.

Oettinger: Can you just stick with the data slide, because that's the one thing you said in this session that in appearance at least may contradict the "no grand scheme" kind of thing. Why do you do that here?

Edmonds: If you remember last year when I came, I talked about JUDI, the Joint Universal Data Interpreter. So did Dick Macke.* That was our quick-fix phase. At

* See Albert J. Edmonds, "C4I Issues," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1994.* Program on Information Resources Policy, Harvard University, Cambridge, MA, January 1995; and Richard C. Macke, "C4I for the Warrior," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1992.* Program on Information Resources Policy, Harvard University, Cambridge, MA, August 1994.

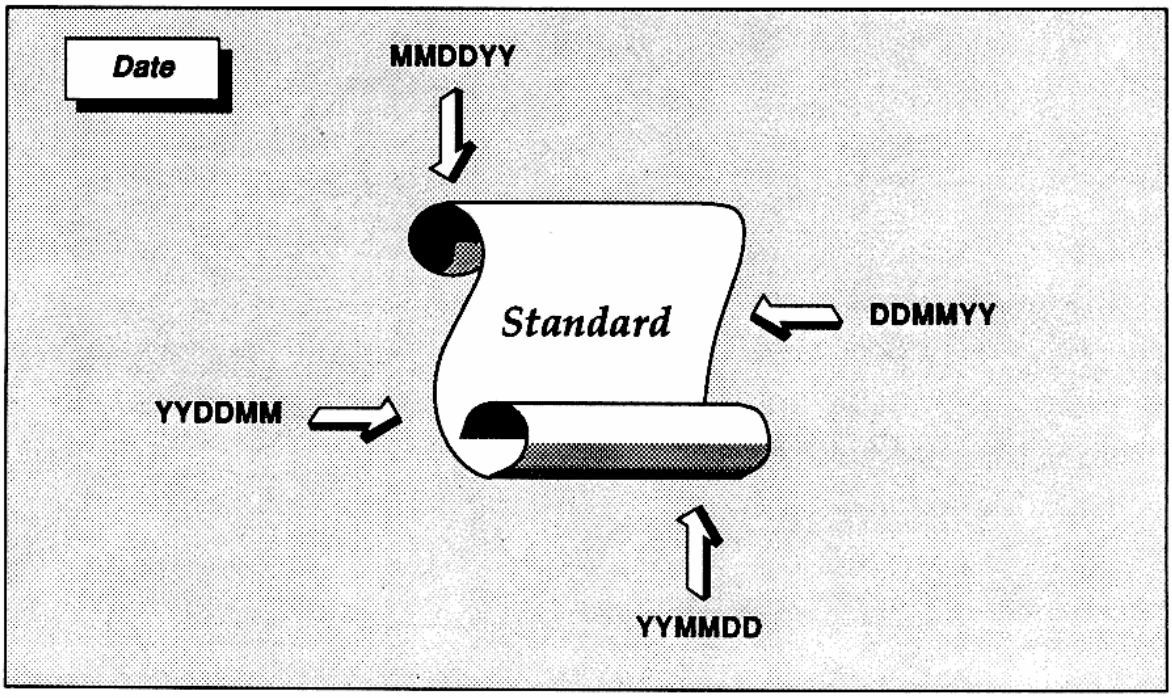


Figure 30
Data Standardization

that time we said, "We don't have time to do standard data and do this kind of TAFIM stuff, because we would need to make some progress and have some success now." So we didn't do that then. We just kind of got an interpreter, a translator, and took four dissimilar systems and let them hook up together and made them work. That was the quick fix. But we thought we needed more technical underpinnings as we go forward.

What we're saying here is that once we take 9,000 of these things—and we think there are going to be about 9,000 or less, because we're going through all the DOD major systems and we found that these are the common data elements—then we'll standardize them so they all have the same structure and the same texture and meaning, and put them in the repository. When you put them in the repository, all we're saying is when you buy or develop a new system, use this as a tool to do your work so that this date will always be your date. If you're going to take an old system and migrate it forward, and you need to do some software modification or engineering, use these things for your tools so that when we go cross-functional, and try to exchange information, it's easier to do. So this still is not a grand design, it's just a tool. Those three things I talked about are really tools.

Oettinger: But you wouldn't abolish the JUDI-type translator?

Edmonds: Oh, absolutely not. As a matter of fact, the logistics guys right now are exchanging information because they're using the JUDI kind of thing. I still think JUDI is the best thing around for the first step. Sometimes it might be the best thing forever, because you don't want to pay for changes on systems that might be too old and might be going away. So you just go ahead and do a translator between them, and call it quits. Say "That's good enough for me," and kind of starve it to death and let it die when it dies.

Student: Sir, would you say that this concept in the future will allow the organization, specifically the armed forces, to have less staff, less support people, and more teeth?

Edmonds: Yes. This (figure 31) is from a briefing I'm going to give when the program people, the budget people, come to see me next week. This is the profile of my megacenter, and you see the slope of it. In 1992 we had 5,580 people running computer centers for us. In 1995 we were down to 2,957. That's just about half. If I take this profile further, I'm going to lights out. Then with all this good technology, I'm going to have five or six people on a shift monitoring screens, and, oh by the way, they can do a lot of this from their houses if you want them to. So you're absolutely going to have a lot fewer people, but they'll all be doing different things. As a matter of fact, what I'm trying to do is take some of these people and put them against the security problem, because nobody has any bodies for those.

Student: Right, sir. That's for your organization. Do you see a core layer, like will a JTF commander need less staff to do the same amount of work?

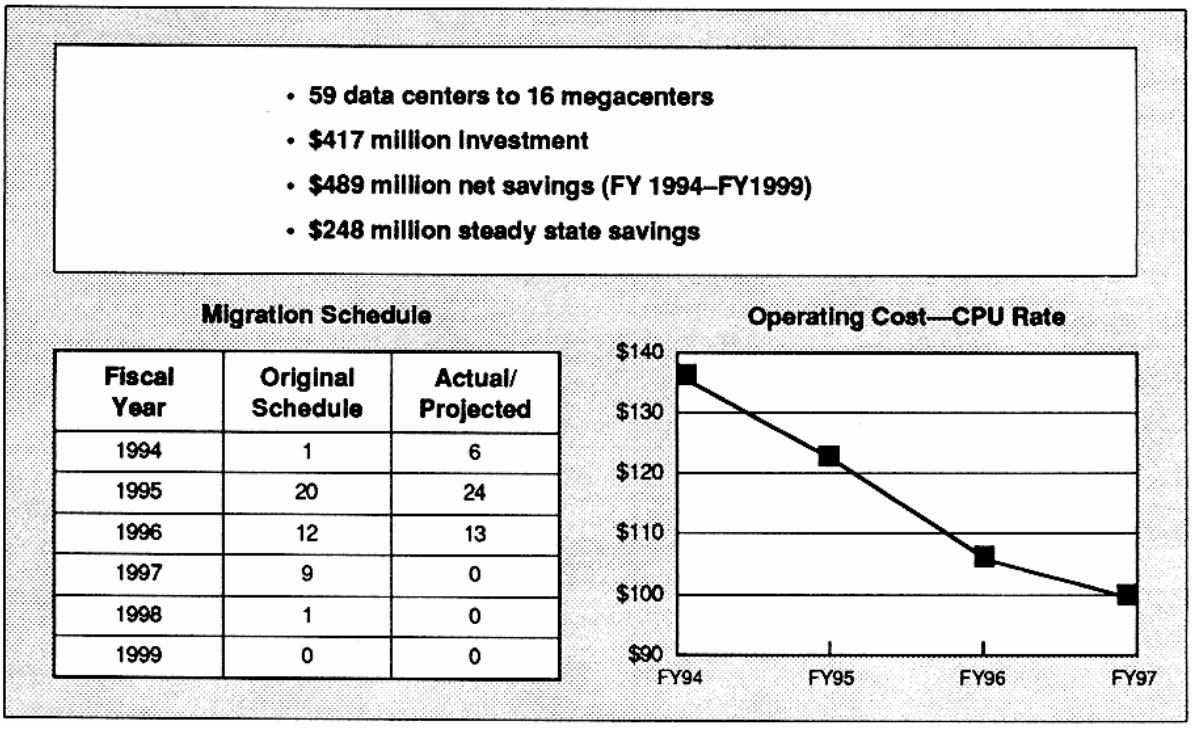
Edmonds: He'll need less staff for sure. He'll have more shooters, because I'll tell you right now, there were 18 guys from the Air Force just to get the air tasking order together, and you don't need those guys. You can put out more from the Air Force and rely more on the system.

Student: General, is it true that the services have sort of relinquished their control of the design of the architecture—the operation and procurement even—to your organization? I mean C4I systems. Have they sort of given the control of this over to DISA?

Edmonds: To some degree.

Student: Standards, architectures ... ?

Edmonds: Standards, architectures, testing, integration; those kinds of technical things. Believe it or not, the best thing (and this is not because I'm saying it) that has happened to me or to this area in the



Fiscal Year	Original Schedule	Actual/ Projected
1994	1	6
1995	20	24
1996	12	13
1997	9	0
1998	1	0
1999	0	0

Figure 31

Megacenter Consolidation

Department of Defense is that I was the J-6 at CENTCOM before I came to the Air Staff. Rick Jensen worked for me over in the Air Staff. I left there and now I'm in the Joint Staff. Those two J-6 jobs out of CENTCOM and on the Joint Staff, gave me warfighter or operator credibility, so they're willing to trust me with those technical things that we always wanted to do for them, but they would never let us do them. So now I can call them up and say, "You know, this system that you have running is really sick."

We did a demonstration the other day for a command and control system. They have 46 applications that still remain on the table. They're going down from 143 to 46, so we at DISA did a model and ran those 46 through the model on jointness and on technical sufficiency. Twenty-four percent of them were not very good, and we presented GCCS. At first we thought we were going into a hostile audience. General O'Berry, who is the Air Force three-star, said, "This is absolutely great!" He said, "You can't ever start doing these kinds of things till you clean up all the garbage you've got around." So now they're going to go back and look at the garbage we pointed out to them and come back and see how much they're going to kill. It would save money, reduce people, and expenses, and facilities, which is all very good.

So this is absolutely a renaissance, if you will, in information technology. This will never be the same. There will never be just communications sitting by itself and automation over here, and something over here, and some other things doing something else. If I were in business to make money today, I'd be trying to get all those people who are fighting to stay separate, to keep it all in their own little stovepipe, in the same room and make them come out as one thing. I can make them come out as information technologists or information warfighters. I'll get them a new MOS (military occupational specialty) or AFSC (Air Force Specialty Code) or whatever you call it where you come from, and there will be a new career field, and they will do all of this, every bit of it. I wouldn't have many other uses for people either, other than supporting those folks. As a matter of fact, you aren't going to need a whole lot of guys with M-16s on the ground other than for peacekeeping and for police actions, because we're going to be able to program missiles on the fly, change the target en route. You're going to be able to show people how much you can hurt them so you don't have to prove it.

I used to say that although we didn't have a feed in Haiti, I wish we had. There's no doubt in my mind that if we had a feed in Haiti with GCCS, I would have shown Cedras a GCCS picture of our capabilities and said, "Frankly, that's what happens." Information is power. If you could show them that they are about to be destroyed right here—there's 60 C-141s, and the parachuters will jump in here, and there's going to be a lot of blood flowing—he should say, "Time out! I don't want to be here. I want to go somewhere else. Can I get some of my money out of the bank and go?"

That's what you want to do. You want to deter. For a long time the only way we could deter was with nuclear weapons. I really do believe we can deter with information—the knowledge of it, the certainty of it. I used to tell my kids when they were growing up, "I would never threaten you with punishment, but the certainty of punishment will keep you from doing wrong. There are two or three things that if you ever do them, you guys will get punished. So don't do them!" That's not a threat, that's the certainty of it. That becomes deterrence. I told them, "I set the standards in our family, and I don't know when I might go off. So don't push me!" That's very helpful.

Student: Returning to your discussion of information security, I'm just very curious. When you look at protecting the information realm, do you see it as being securable in the future, or is the info realm going to be an area where offense gains a permanent upper hand, like something in biological warfare?

Edmonds: Selective protection. I use an analogy. I say, "Get on the information highway, but make sure you fasten your seatbelt, close your windows, pay atten-

tion, and watch your speed limit. Because if you don't close your windows, anything will get in. If you don't do your seatbelt right, and you hit something, you'll go through the windshield. Watch your speed limit, because if you go beyond what the law allows you to do on this information highway, you'll be in trouble." That's the advice I give. But I think they'll do selective protection.

Student: You do see it? Do you think we will be able to compartmentalize parts of it and fully secure it?

Edmonds: We have no choice. The infrastructure of this nation will have to have protection in it eventually, when we find out how to afford it and how to do it by e-mail one byte at a time. I think that is what we have to do. We can't make a big pronouncement about it. You can't go out and put headlines out on it. But you have to tackle it, and that's part of my job.

Oettinger: Sir, we are very, very grateful to you. I want to get you out of here by a quarter of four. We have a modest token of our appreciation. Take it with you and enjoy. And thank you, thank you very much.

Edmonds: Thank you. That's very nice, Tony. It was a pleasure.

INCSEMINARS1995

ISBN-1-879716-29-1