Seminar on Intelligence, Command, and Control

Defense Science Board Recommendations on Information Architecture for the Battlefield
Robert A. Rosenberg

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

January 1997

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

Defense Science Board Recommendations on Information Architecture for the Battlefield

Robert A. Rosenberg

Major General Robert Rosenberg, USAF (Ret.) is Executive Vice President and General Manager, Washington Operations, of Science Applications International Corporation (SAIC). Before retiring from the Air Force, Gen. Rosenberg was Director of the Defense Mapping Agency from 1985–1987, and from 1983–1985, he was Vice Commander in Chief of the North American Aerospace Defense Command and Assistant Vice Commander of Air Force Space Command. He served as Assistant Chief of Staff for Studies and Analyses, Headquarters, USAF, from 1980–1983, and from 1976–1980, he was a member of the National Security Council, where he served as advisor to the Assistant to the President for National Security Affairs. From 1974–1976, he served as Deputy Director for Programs, Principal Deputy, then Acting Director of the Office of Space Systems, Office of the Secretary of the Air Force. Gen. Rosenberg has also managed the USAF Operations Research Center, and served as U.S. delegate to the NATO Advisory Group for Aerospace Research and Development. Gen. Rosenberg received a B.S. degree in general engineering from the U.S. Naval Academy, an M.S. in aerospace engineering from the Air Force Institute of Technology, and graduated from the Industrial College of the Armed Forces.

Rosenberg: I really am not quite sure what the good Doctor O. told you I was going to talk to you about. So before I put any slides up, let me tell you a bit about what we're going to talk about today. I have been helping DOD for many, many years in the C³I and military space business. It's kind of a love/hate affair. When I was on active duty, I spent probably too many years in the National Reconnaissance Program and in the military space business. I failed at attempting to run the Defense Mapping Agency (DMA) on my last assignment while I was on active duty. As kind of a penance for all the things I fouled up when I was on active duty, Bill Perry and Paul Kaminski* have had me serving on a variety of Defense Science Board (DSB) task forces over the past few years.

I sent Tony a copy of the study called "Information Architecture for the Battlefield" because, having helped be a father and mother of your course, I thought it was important. I was commenting to one of you that Tony and I colluded to persuade the Air Force to fund Air Force officers' participation properly. But at any rate, knowing the

genesis of the course you all are in, I thought it was important that you understand that every time you hear a Bill Owens or a Shali or somebody else talk about information dominance of the battlespace, that it came from this study. These are the founding principles that led to many things that are happening today in the Defense Department, such as the invention of the C⁴ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) JROC (Joint Requirements Oversight Council) and JWCA (Joint Warfare Capabilities Assessment). If I'm using buzzwords that you don't understand, stop and say, "Hey, what does that mean?" But I'm going to show you a vugraph that's the genesis of Bill Owens starting that piece of the JWCA. As a matter of fact, we now have tools out there to do incremental value-added analyses of whether we should invest in this and invest in that and so on.

I'm going to give you a kaleidoscope presentation. I'm using vugraphs from three different Defense Science Board task forces.

The beginning was the DSB Task Force on Information Architecture for the Battlefield, August 21–September 1, 1994.

I wanted you to know that because a lot of the decisions being made today in OSD (Office of the Secretary of Defense), in the JCS, in DISA, and (with some heel-dragging) in the military departments in the world of C^{4}I and so on come out of the paradigm that was first articulated in a coherent way in this study.

As we were moving along, trying to articulate what had happened in this study, and as we were trying to figure out how to implement it, we tripped across the fact that the old world of maps, Magellan's world of maps, isn't very helpful. We are building a Tower of Babel out there in the world of C^{4}ISR. For the third task force I was on (which I have no vugraphs on because they're all Secret, and I've got to brief you at the unclassified level), I was sent over to the Bosnia theater by Secretary Perry to help make a difference on putting 20,000 people on the ground. I saw targeting come out of the JAC (Joint Analysis Center) in Molesworth that often were different from the coordinates being used at Vicenza and Aviano and aboard the *Teddy Roosevelt*. As I said, it's a Tower of Babel.

As we were tripping our way down this, a second study was turned on that said, "Tell us what we need to do in the national security arena about getting our act together in the world of geospatial information"—not maps, but geospatial information—a new buzzword that you're going to have to learn more about. So the second study is about Defense Mapping for Future Operations. They were kind of integrated with each other, and that's the way I'm going to brief them.

Then, as I said, there's the third study, which I'll do some ad libs on. About three weeks after Scott O'Grady got shot down, Secretary Perry called four of us into his office and said, "I'm really unhappy. Every time I ask, 'Did O'Grady need to be shot down?' and I push, I get mush back from the community for an answer. And every time I ask why it took five and a half days to get him back, and I push, I get mush for an answer." He told us to go over to the theater and chop up the turf, destroy the NIH (not invented here), take a meat ax to roles and missions issues, and come back with some dramatic recommendations on how to make information to our warriors much better. He asked us to look at expanded operations, because at the time it was Deny Flight—40 sorties a day—to unsuccessfully keep 21 Bosnian Serb airplanes on the ground. He asked us to look at 20,000 U.S. people on the ground, principally a peacekeeping operation that could escalate into peacemaking, and could escalate from there into either armed withdrawal or warfare. Some members of this four-person task force were people who had participated in the other two studies. This was implementation of the concepts and ideas that came out of the first two. So that's an overview of what we're going to fly through either at 20 knots, or Mach 15, or 30 miles an hour, depending on your perspective. Please feel free to interrupt as we go along.

The DSB Task Force on Information Architecture for the Battlefield was a year-long effort (figure 1). The way the national security community operates in terms of science boards is that there is an Army Science Board, a Naval Studies Group, Air Force Science Advisory Board, and a Defense Science Board. By the way, my good friend Tony here served on a lot of prestigious boards that operate the same way, such as the National Academy of Science. In many cases, the science boards don't invent anything. What they do is take terms of reference—a problem where their sponsor says, "I've got a problem. I want you to go solve this problem for me." So you go out and spend almost a year on each one of these studies, surveying what's going on out there, and then integrate all that information, come back to the decision makers who asked you to look into these problems, and try to give them your best recommendations. So with a lot of what you're going to hear in here, those of you who have grown up in DOD are going to say, "What's new about that? I knew that all along." Well, no, you didn't know it in the integrated fashion that the Secretary of Defense finally got exposed to.

Student: How much cooperation do you receive from the people whom you are trying to study? Is there resistance?

258

- **Identify and recommend information architecture to enhance combat operations at all force levels**
  - Assess current/future DOD and service plans
  - Develop concepts for information flow on the battlefield
  - Develop architectural approach to support these concepts
  - Consider policy/security restrictions through software/encryption rather than hardware/separation
  - Consider how joint exercises, gaming and simulation can validate alternate concepts
  - Provide specific guidelines for implementation of recommendations
- **Focus on information support to theater or Joint Task Force (JTF) commander**
- **Information architecture includes**
  - Operational concepts
  - Information concepts
  - Networks, databases, system security and necessary software

Figure 1

Defense Science Board Task Force on Information Architecture for the Battlefield (August 21–September 1, 1994): Terms of Reference

Rosenberg: Yes, there is resistance. There's a lot of NIH, and, as a matter of fact, I'll point out a few cases of that. Remember, we're all victims of our backgrounds and our environments, and we're very comfortable in those. On the second study, where we talked about using commercial and international remote sensing satellites to provide warfighting data to our armed forces, it made the current providers of highly classified overhead reconnaissance imagery unhappy, because they think they are the only people in the world who know how to do it, and yet they're not in tune with the modern commercial world. But then, their leadership was very enlightened; as a matter of fact, their leadership directed the implementation of many of the recommendations.

When we went over to Bosnia, a lot of people didn't want us there. "We don't want your help. Stay out of here!" When I went into JAC Molesworth and I asked the colonel, "Show me how you are searching for, locating, and targeting mobile artillery," she said, "That's not my job." I said, "Then you're not very relevant. I don't know what this place is for if it isn't to do that." One of the studies that Secretary Perry gave us when we went over on that trip was an Army historical document

about the occupation of the Balkans by the Germans in World War II. The Germans lost one in seven "peacekeepers" to guerrilla warfare. So we're going in there, putting 20,000 people on the ground, and we've got to worry about shoot-and-scoot artillery. That colonel in JAC Molesworth needs to be paid to worry about that. But it wasn't her fault, because the policy maker level above her refused to acknowledge that we were going to have a peacekeeping mission. There's always a cause and effect for these things, so the fact that somebody didn't want to do a particular job was explained by, "Well, she didn't think that was in her rules of engagement job description." There's always a good reason why people don't want to cooperate—at least a good reason from their vantage point.

Back to this first study (figure 2). When I was on active duty, we built a lot of Cold War command and control systems. They were all stovepiped systems. We had command and control systems over in EU-COM that were going to fight the Fulda Gap war. You didn't have to talk to anybody else. Air Force command and control systems didn't integrate with Army and Navy command and control systems. As the Vice Commander and chief of NORAD, I had command and control systems that let

259

- **Make the warfighter an informed consumer.**
- **Warfighters need to change information systems to accomplish different missions.**
- **Our information systems are highly vulnerable to information warfare; so are our adversaries'.**
- **Buy commercial products, buy commercial services, "buy into" commercial practices.**

Figure 2

Key Findings and Observations

us communicate up over the North Pole, and when the Bear-Hs were coming over we got ready to go back against them. Then we had the NORAD command and control system that told us at Cheyenne Mountain that 10,000 warheads were coming and the President got to tell CINCSAC to create mutually assured destruction. None of these systems worked with each other, nor did they need to, and they all kind of went from the land, naval, or air commanders up to the National Command Authority. We never seriously addressed command and control and communications between Joint Task Force commanders down to their shooters. That's what this first study was all about, because the world actually changed after we won the war against the Evil Empire. I'm going to show you why it becomes far more important for JTF commanders to talk to their shooters.

We were asked to identify and recommend information architectures to enhance combat operations at all force levels; look at what was going on in the DOD and the service plans; develop new concepts for information flow on the battlefield; develop architectural approaches to support those concepts; look at how policy and security restrictions impact our operations; look at joint exercises, gaming, and simulation in this new world of Hollywood coming to the battlefield—virtual reality, simulating the warfare, or its operational aspects, and we were asked to focus on information support to JTF commanders down to their shooters. We were also asked to look at all of it, starting with a clean sheet of paper.

We had retired senior warriors: Bud Edney, who had been CINCLANT before

he retired; Carl Stiner, who was CINCSOC before he retired; Mike Carns, a senior Air Force warrior; and Jerry Tuttle, who was kind of legendary in the C⁴ISR business. Those were the kind of folks who participated in this, and after 50 vugraphs, this is the final chart (figure 2), so, we'll start the briefing with the final chart. We concluded that while Goldwater-Nichols says that joint, unified commanders are supposed to be setting the stage for their prioritized requirements, that can't be. You've got laws that say that's the way it's supposed to be, but they really don't understand the world of C⁴ISR, other than what they're doing today, to the extent that they can sensibly play in the process of deciding how C⁴ISR systems can help them do their job. So, one of our key findings, observations, and recommendations was to strengthen the joint warriors' capabilities to be involved in that decision-making process.

The second is the most important bullet in the whole study. The best way I can describe it is to say that during the Cold War, we were going to send the 101st Airborne Brigade somewhere, and we were going to send a wing of F-15s, and we were going to send a carrier task group with a MAU (Marine amphibious unit). Well, in this new modern world, every single ad hoc Joint Task Force is a kludge of a unique set of tanks, ships, planes, and warriors to do a unique, odd job. It's not the Fulda Gap war, and, oh, by the way, it's not an Iraqi invasion of Kuwait either. That's the wrong war to study, too, if you're trying to figure out how to do this. We may just send a battalion or a company. We may send a flight of four. We may send one

submarine. Again, depending on the mission, it's a kludge of the right tanks, ships, planes, and warriors, and what they need in the world of C⁴ISR is not all these huge stovepiped capabilities we built to fight this big set piece warfare against the Warsaw Pact and the Soviet Union, but instead, they need to be able to (think information technology) think C⁴ISR, take the right sets of hardware, software, information databases, sensors, and comm pipes, and tie them all together to support that particular ad hoc gaggle of warriors. So, in each case, the C⁴ISR suite has to be different.

Those of you who grew up in the military say, "That's impossible. We have to fight the way we train." Right! We have to catch up with the plumbers, electricians, and carpenters, who have all accepted commercial standards as a way of being able to plug and play. That's where the concept of plug and play comes from. Those of you who have been down in Washington know about Hechinger's, the hardware store. Even though I'm not a plumber, I can go in and I can get a standard commercial fitting to fix my toilet, and I don't have to train for it, because I'm going to take advantage of what's out there in that modern commercial world. For those of you who had lunch with me, you already heard that lecture, because our technology in DOD, in the IT world, is 20 years behind where the commercial world is. We talk about investing $100 million in advanced R&D. The Bill Gateses of the world are gambling 10, 20, or 30 times that.

Oettinger: May I inject a thought? You may pick it up now or maybe defer it to later. I hear you almost implying that no training is needed ...

Rosenberg: No.

Oettinger: ... but the commercial world is moving pretty fast itself. The plumber analogy is a bad one because that stuff is pretty stable, whereas most of the stuff in the commercial world is not.

Rosenberg: It's an overstatement. By the way, the plumber's world is changing. The commercial standards do change. But

you're right, and I have a chart in here that talks about the fact that DOD needs to totally change its acquisition rules for the acquisition of information technology. Again, we're victims of the Acquisition Corps. But you're right.

Let me leap forward, because you do raise a good point. When I was briefing a piece of this study to the JROC, or the pre-JROC (the JROC is the four-stars; I was trying to make the two-stars and the O-6s smart before their principal officers) ...

Student: Could you spell out JROC?

Rosenberg: Joint Requirements Oversight Council. They are the Joint Chiefs of Staff senior leadership, who decide where the budget money is going to be spent on buying added capability for our armed forces.

Oettinger: For further details, read Admiral Owens' presentation in last year's proceedings.*

Rosenberg: Now, in this outbrief, when I was talking about the geospatial information portion of this briefing I'm going to give you, an Army colonel said, "General, that is absolutely crazy." What I was saying was that we are going to put in the hands of 7-level NCOs and lieutenants (you're going to see this in the briefing) the capability to build their own finished products out there in their workstations on the back of their Hum-Vee, or in their command and control center, so they can go do their jobs. This colonel said, "That's crazy! You've got to be a mapping, charting, and geodesy expert to do that." I looked out at the audience of about 50 people and I said, "Colonel, I thought I was the only senile person in the room. I suggest that I'm not talking to you. It's too late to save you, because you're too old to understand how to use a computer. Now what I want to do is take you down to

* William A. Owens, "The Three Revolutions in Military Affairs," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1995.* Cambridge, MA: Program on Information Resources Policy, Harvard University, January 1996.

the Pentagon City arcade, and I want to show you your 13-year old sons and daughters interacting in the arcade with the wargames, dynamically fighting and changing things almost at the speed of light. And, oh, by the way, if you'll go home this evening and sit down next to your 16-year old flying cyberspace through America Online, out there channel surfing cyberspace and gluing together all kinds of software packages, that's whom we are talking about."

That's my answer to your question. No, it's not plumbers, but the reason they can do that, and the whole concept of the spiral acquisition process of buying modern information technology for DOD, derives from the way the Internet has become maybe not really consumer friendly right now, but for anybody who wants to plug into it, you've got to have open system capability or it's Greek transferring to Hebrew, and it won't work. So, what we're trying to do is make sure that the stuff will work together.

At any rate, the second bullet is the heart of the presentation. As a matter of fact, we gave it a title: that we need "enhanced reconfigurability."

Student: Why didn't you just stay with "flexible task organization?"

Rosenberg: Because that's not software or hardware.

Student: In IT terms?

Rosenberg: You're right. That's what we're talking about, in IT terms—it's flexibility.

The third issue is that as we become more and more dependent on the world of information to support our military operations, we become more vulnerable. That's the bad news. The good news is that our adversaries are using the same stuff, and so that's a business opportunity to kill them.

Oettinger: Before you go on, can I go back to just the previous point for a moment, because the notion of flexibility and so on is kind of neat, but it implies that certain things are really quite standardized.

Let me make a statement and then you can argue or postpone the consideration. Often, that happens only at the lowest level of standards. You talk a lot about the Internet and the World Wide Web. One of the key reasons why the World Wide Web exists and works is that somebody decided that they were going to squander a great deal of processing capability by having only seven-bit ASCII—it's the most rigorous, elementary standard you could imagine—used in the communications from one place to another. Now what does that imply? It implies that both at the sending and at the receiving end, you've got to have a lot of processing. What that means in practice is that at both ends you've got a lot of idiosyncrasy. Now, as a user, you can plug and play into the World Wide Web, but that is not exactly the same thing as the guy sitting in front of a screen having any kind of standardization. If you look at going into the Web and a lot of the sites you reach, many of them require you to figure out what the hell's going on because you're in some alien world. So the question is where that standardization and where the plug and play are on some level from a user's eyeball and brain, or down to the bowels of the techie.

Rosenberg: We call it DISA. We call the architect, an organization called DISA, which is responsible for establishing standards within the Defense Information Infrastructure.

Oettinger: Yes, but that's not necessarily the same as an eyeball standard at the point where ...

Rosenberg: But it's far more flexibility than we've got today. I'm going to show you the concepts. You're about 20 charts ahead of me.

Oettinger: I don't want to throw sand in your gears, but come back to it later.

Rosenberg: I'm going to show you the kind of flexibility that he's talking about. The Defense Science Board, understanding the technology that is available today and within the next 5 to 10 years, felt there was

not a problem doing what we proposed. As a matter of fact, over in Bosnia we are demonstrating many of the things I'm going to show you here.

This last bullet was aimed at the fact that even though Secretary Perry and Deutch and White* and everybody talked big about acquisition reform, and about best commercial practices and standards and so on, the DSB was critical of its implementation because all of those acquisition reforms are aimed at weapons systems and systems that have 5- to 50-year life cycles. In the world of information systems, the speed of change is one-time throwaway to six months to two years dramatic change in capability, and while acquisition reform attacking 5- to 50-year life cycle systems is good, it doesn't have anything to do with taking advantage of what's going on in the world of commercial information technology. So we said, "Change that. Do something about it."

I'm only going to brief you on part of this study because of time, and it's all in a document. But I did want to show you the way we went through it. We were organized into a warriors panel, an information warfare panel, an architecture and technology panel, and a business practices panel, and we tried to integrate all that into an integrated set of recommendations from that two-week effort we sat in together (figure 3). Key to starting this task force's view of the world was to ask, "What's different about the new global security environment and its changes to the baseline?" We don't have that nice comfortable Evil Empire anymore. We've got a whole world of new paradigms for the use of military capability in supporting national security objectives that we never thought of in the good old days, ranging from peace to war, and far more dependence on interface between the civilian world and the military information systems world.

With that in mind, we felt we needed to look at what we could do to dramatically improve what the joint warriors have in their hands, and what we can do that would lead to information dominance of the bat-

tlespace. And you don't have information dominance of the battlespace, even if you can see everything and hear everything and know everything. We can sit here with a chessboard in front of us and you and I both have information dominance of the battlespace. We both know everything about the battlespace. We have instantaneous logistics support. Why is it the chess master keeps whipping me all the time? He's the chess master, and there are 30 chessboards out here. We all have information dominance of the battlespace, but he keeps beating all of us. Why? Because he's practiced and practiced and practiced and practiced, and been killed many times on the battlefield.

Part of the concept here is that we want the warrior to be able to get killed many, many times on the battlefield. That's the introduction of the concepts of marrying distributed, interactive modeling, simulation, and wargaming into this new environment so that it's safe to die. Now, those of you who have been in combat probably question how realistic you can make that, but I'm going to talk about some examples as we go along.

As a matter of fact, I'll just get out in front because I want to make this as informal as possible. One of the things we saw when we were working the problem of how you put 20,000 people on the ground over there is that it would have been nice to have had a ground-level and a top-down view, a 3-D view, a virtual reality view, of the battlespace. I've got to tell you, it makes a lot of difference if you're going to drop the 101st Airborne Brigade onto a very artificial 3-D view of the earth, like what we have through our defense mapping capability today, which says, "There's no place for snipers to hide." In fact, if I had virtual reality, I could see that I could lose the whole 101st on the way down from hidden snipers, AAA (antiaircraft artillery), and so on on the ground. So, "virtual reality" means "virtual reality" to the warrior. He wants the real thing. Those of you who saw "Clear and Present Danger," do you remember the convoy going through the urban scene and blam, they start getting shot at? That was a mandatory movie to go

---

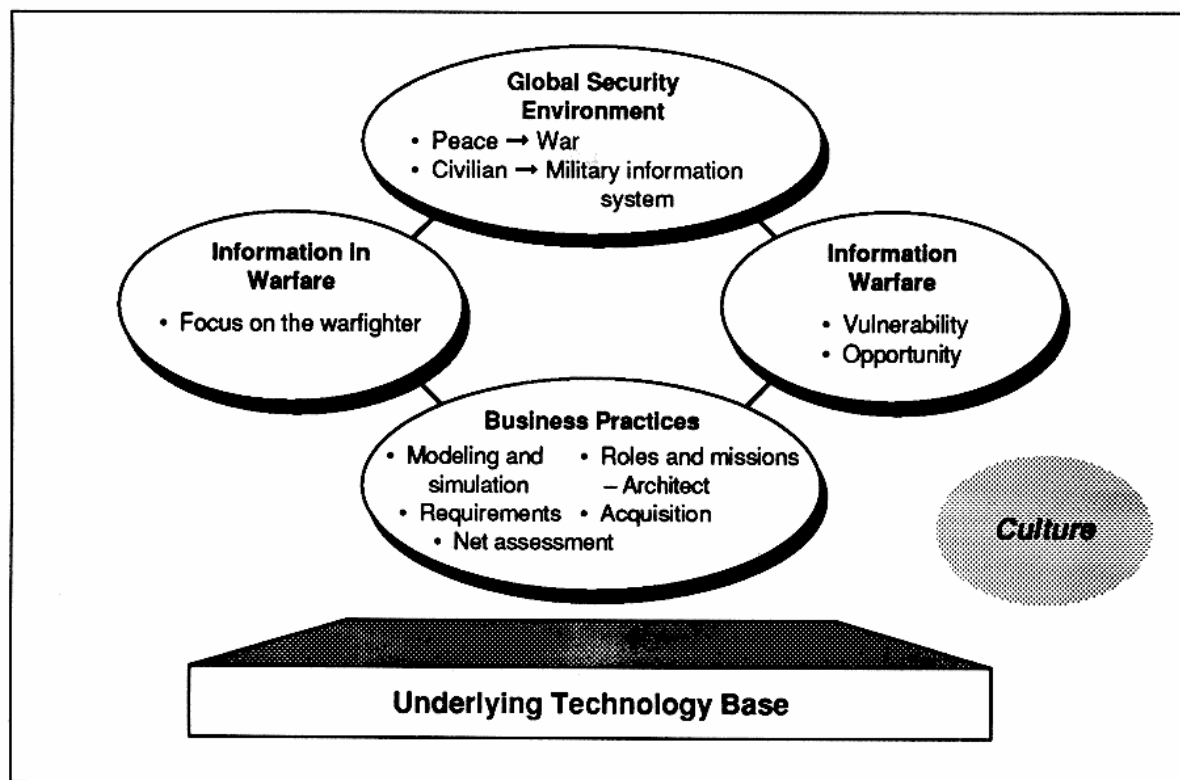* John White, Deputy Secretary of Defense.

263

Figure 3

Task Force View

see during the summer study, because we need to be able to create that virtual reality so they can practice driving down the street. In the good old days, we didn't do urban warfare. That's a new military mission. We liked fighting the Fulda Gap because we didn't have to fight that one. We really are fighting urban warfare now.

Student: Some of us did it in 1968, sir, if you'll remember back, in a couple of cities there.

Rosenberg: Yes, I used to provide the digital maps for General Stiner when he had to go in and get people out. Looking at this technology base to support these concepts and some new business practices was all part of the way we approached this.

I've talked to this chart already several times (figure 4). I said we're not fighting this Fulda Gap war anymore. This—operations other than war—is the war we're fighting. The important numbers here are, first of all, that as long as an administration thinks the risk is low, the probability of our

doing these things is high, just as they thought the risk was low in putting 20,000 people on the ground. Secretary Perry was a lot smarter than many politicians who were advising the President, which is why we went a lot slower, and we got a lot more careful. The point is that more and more, now that there's no bipolar world (I'm not going to lecture to you about what happens in a monopolar world), we truly are being called on to do all kinds of things we never thought of doing before. The important numbers are that between Vietnam and the fall of the Berlin Wall, there were only 20 such operations other than war, and between the fall of the Berlin Wall and today, it's 70+ and counting.

This is a way of life. It's a way of life for our military, and different military situations demand different plug-and-play capabilities. This means that kludge. This means a different set of tanks, ships, and planes, and warriors to do each one of these. In each case, they need different sets of hardware, software, information databases, sensors, and comm pipes to
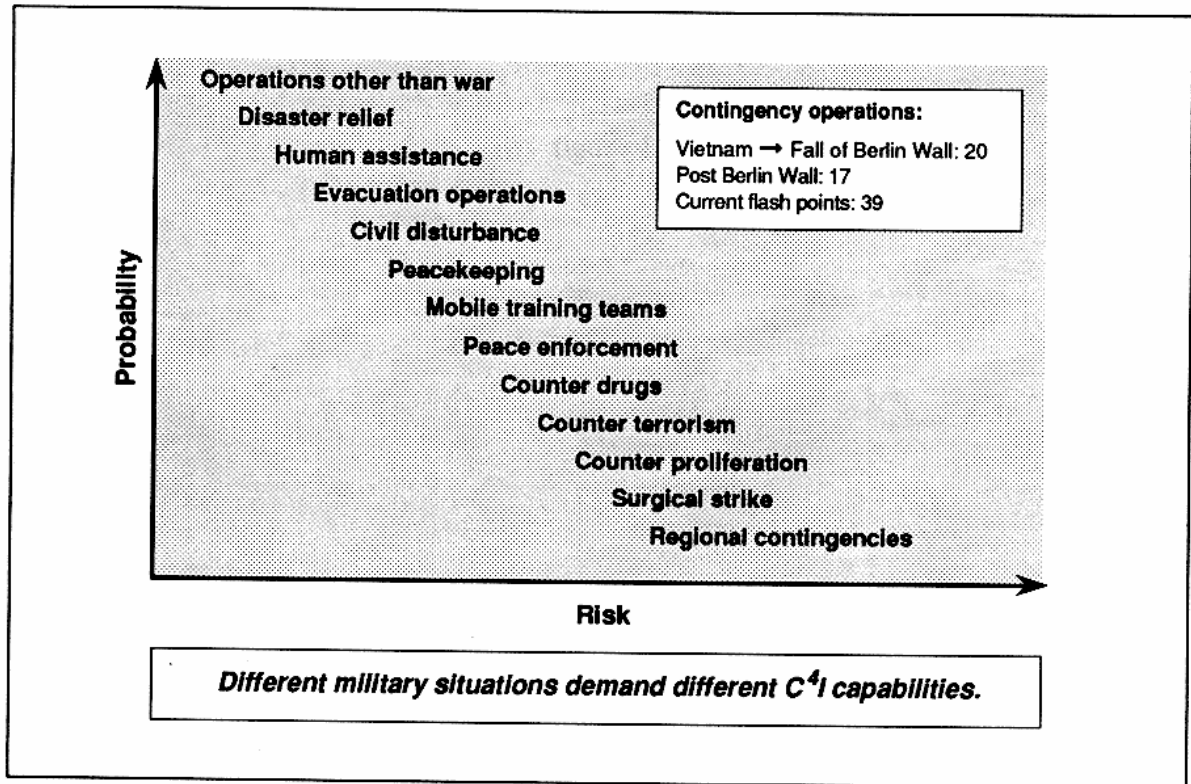
Figure 4
Military Operations Continuum

support whatever ad hoc gaggle of shooters gets sent out there to do this stuff.

This is what we heard during the year-long course of this effort (figure 5). Was Bill Owens here?

Oettinger: He was here last year, but they've read his presentation.

Rosenberg: Bill talks very articulately about joint operations, and we're working very hard to make that happen. My company happens to be the integrator for the Global Command and Control System (GCCS). We also do the Army's command and control systems, the Navy's command and control systems, and the Air Force's command and control systems, so I know first-hand that we are a long way away from joint systems. This (figure 5) was a chart in the study that said, "What we heard was that the Chairman of the Joint Chiefs of Staff is totally committed to joint C⁴I for the Warrior." (This shape is a cornucopia of plenty.) The core of that is called GCCS.

We listened to the Army, Navy, Air Force, Marine Corps, and defense agency folks get up and tell us how their systems were going to get us joint C⁴I for the Warrior better, cheaper, faster. We heard Lee Hammarstrom* come in and tell us how his Global Grid was going to get us joint C⁴I for the Warrior better, cheaper, faster. We heard all the program managers who are in the distributed interactive simulation business all the way from Fort Leavenworth down to USACOM's joint training and exercising stuff to ... you name it. They'd say it was going well, and ACTDs (advanced concept technology demonstrations) are all going to do it too! You notice that the straight left-to-right arrows are much heavier than the centripetal arrows. So our message to the SECDEF was, "Left to our own devices, the separate military department and defense agency organizations will

---

* Lee Hammarstrom, Director of Research, National Reconnaissance Office.

265

Figure 5
What We Heard
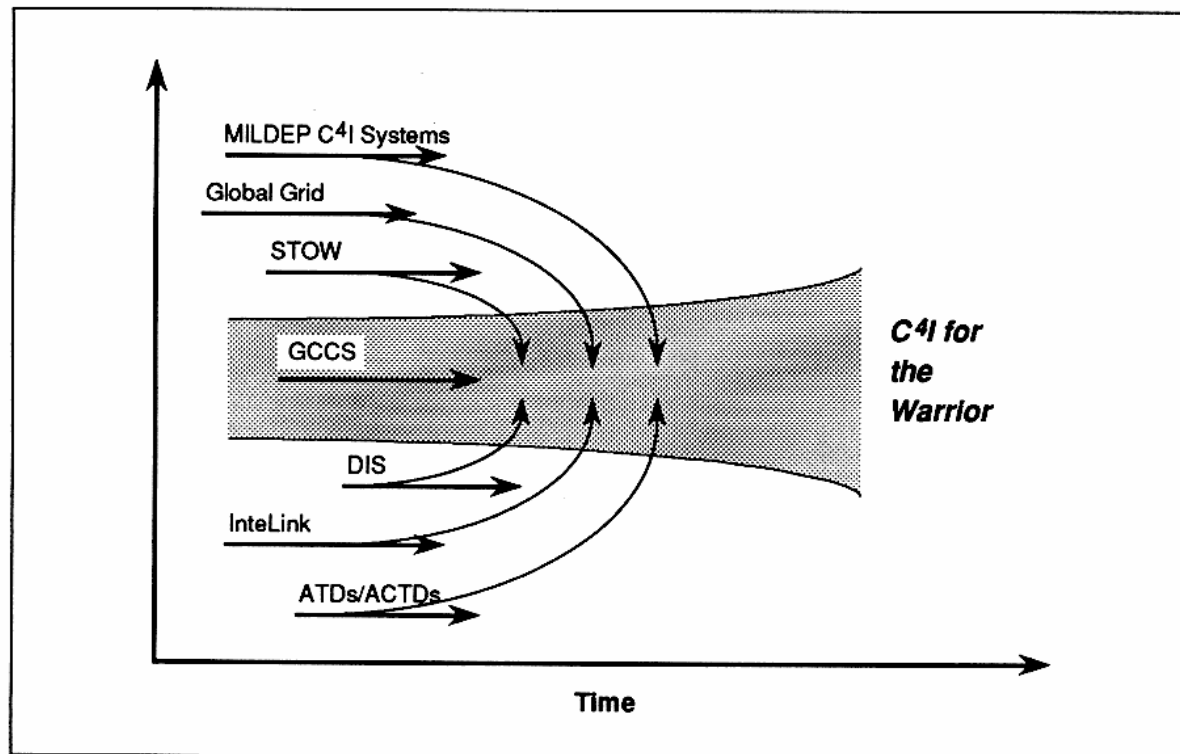
STOW = Synthetic Theater of War

not do this. To do it, you need to institute positive incentives, not the power of 'no,' which the Pentagon is famous for, to make PEOs (program executive officers) and the folks who build these kinds of systems want to integrate their capabilities."

My favorite example, which General Franklin gets pained at every time I use, is that when I go to the PRISM Rapid Prototype Center out here at Hanscom AFB, that's not relevant. It's a command and control prototyping place. Actually, he's changed it a lot. But when we first looked at it we said, "That's no good." It's no good because, first of all, it does rapid prototyping and we're at the state of the art in information systems where it could be rapid development. The second thing was that no warrior has ever set foot inside it. What we want is the ability that when they put a new element of command and control capability in that Rapid Prototype Center, milliseconds later, it shows up on the workstations of the 7th Air Force warriors in Korea and up at CINCUNK's

(Commander in Chief, United Nations Command) Headquarters in Seoul, and out at General Tommy Frank's 2nd Infantry Division up in Wujongbu, and they bring in from the worldwide synthetic theater of war world a virtual reality war against North Korea, and they fight it. When it's over, if they like that new command and control software, it becomes operational. That's the world we want to get to. That's the world of Internet. It's that world of those 15-year old kids sitting there unencumbered by the discipline of the outdated defense acquisition process who don't have to obey rules. They just go out there and pull in whatever tools and capabilities, and they go build their enhanced kludge.

Given a snapshot of what we can do to enhance information in warfare, or information dominance of the battlespace, we're joint everywhere (figure 6). We said, "What the joint tactical commander really needs is timely information to achieve decisive advantage on the battlefield. He

266

needs total situation awareness, not just red. Fratricide is very serious.

I watched 24 aircraft take off from the *Teddy Roosevelt* on the first strike to drive the Bosnian Serbs to the peace table. Twenty of them came back with a full load of stores. The reason was they couldn't meet the tight rules of engagement for weapons release. When an SA-6 surface-to-air missile battery lights up in a Bosnia theater, you can't tell whether it's an Albanian SA-6, or Bosnian, or Serbian, or Macedonian. You can't tell whether it's a good or bad guy; it's an SA-6. Not only that, they all speak the same language. There are Texas accents, and there are New York accents, but it's all the same language. So providing total situation awareness is far more than the set-piece battlefield of knowing what's on the red side of the Fulda Gap, and what's on the blue side of the Fulda Gap. It's a lot more information than we have today. What General Hal Hornberg* needed most over there was combat information he could act on. He needed an underground, three-dimensional view of the integrated air defense system cabling system so he could cut it. We need delivery to decision makers and weapons holders responsive to the JTF commander and below, tailored to warriors at each level. I'm going to talk to you about a military CNN.

Today, in the judgment of the Defense Science Board, the warrior is saturated with data and starved for useful information. What we were looking for were concepts to provide him useful information and effective, but not restrictive, security. We said that we must change the Cold War paradigm of NSA and CIA with big walls of security, and instead move to risk management and vulnerability management.

In this new world of operations other than war—a lousy name, because it is all warfare—the warrior requires expanded capabilities. Let me talk about some of them (figure 7).

All of the joint warriors we talked to said they needed to expand their capabili-

---

* Major General Hal Hornberg, Deputy Commander 16th Air Force, Aviano, Italy.

ties, but they couldn't. What does that mean? It means that the JTF commander needs to be able to interact collaboratively with his land, naval, and air components, using their modeling, simulation, and wargaming capability to "what if" the battlespace before they ever deploy. Remember, there is no ops plan 5105 or 4102. This is a new world. We don't have this set-piece world to rehearse against over and over again, because it doesn't exist. We don't know what we're going to do, except we're going to put 20,000 people on the ground over there.

If the land component commander can work with his wargaming capability, tied back to Fort Leavenworth at the National Training Range and wherever else, emulation, simulation, and virtual reality can be brought together. We want to look at what happens if we're going to drop in the 101st Airborne Brigade, and instead of being unopposed, there is sniper fire. There are SAMs (surface-to-air missiles) against the C-17s and the C-130s. If the harbor is mined, and we can't go in with an amphibious landing, what are we going to do instead? These warriors need to plan together collaboratively for this peacekeeping operation, and by the way, once they get on the ground, they need to continue planning it, because what happens tomorrow if there is a major break at the peacekeeping line, and we have to turn it into a peacemaking mission instead? So the new substitute for the now-nonexistent ops plan is to be able to do operations planning before deployment, on the fly, and in split-based operations, while a lot of your infrastructure is still back in CONUS and you are deploying to the theater. You still have to have tethered interface to keep up with the tempo of what's happening.

Student: Excuse me, sir. Could you go back one slide for me? I want to look at the bottom again (figure 6). You skipped over the part where we talked about disrupting the enemy's information. You were talking about operations other than war. It occurs to me that there are times when that's the last thing we'd like to do; for instance, if

- **Timely Information to achieve decisive advantage on the battlefield**
  - Provide total situational awareness—enemy and friendly
  - Dominate all levels of battlespace
- **Rapid movement of actionable combat information**
  - information necessary to fight forces
  - Reliably, real-time
- **Delivery to decision makers and weapons holders**
  - Responsive to CINC/JTF commander and below
  - Tailored to the warrior at each level
  - In usable format
- **Effective but not restrictive security**
  - Confident protection
  - Graceful degradation
- **Information warfare as a major discriminator**
  - Deny/disrupt enemy's information
  - A force multiplier
  - Accelerate conflict resolution

Treat the warfighter as the informed customer

Figure 6

What the Tactical Commander Requires

I'm a commander on the ground in Bosnia, and I'm worried about Bosnian Serb local militias getting out of control. Yet you say that the operations other than war isn't a really good descriptor, because it's all warfare. I'm wondering, aren't there cases where that's not exactly what we want to do?

Rosenberg: I didn't say we *always* want to do that. We need to have the capability to do it. We do want to disrupt. We may want to provide him misinformation. On the other hand, we may want to make sure he knows exactly what is going on. We may want to make sure there are very clear lines of communication with the opposition so that they know what will happen to them if they do something wrong.

Student: So, can you imagine situations where we might actually, in a situation like Bosnia, want to help the Bosnian Serbs with their lines of communication?

Rosenberg: Sure, absolutely. As a matter of fact, in this new world we're facing, where we're talking about sharing the same satellites with the enemy, I can't shoot them down with a physical ASAT (antisatellite) interceptor. That would be stupid, because I'm depending on them too. Maybe what I want to do is feed them misinformation through that satellite. I want to mask what they're getting. Did you see the movie "Speed"? Remember, the bad guy was going to blow up the bus, and so we fed him misinformation so he thought everything on the bus was going the way he wanted it. Information warfare is a major discriminator. There's an example of something out of the world of Hollywood. That's a good paradigm to talk about.

As we were tripping down the way watching all this happen, we said, "Wait a minute! We've got a problem with this whole concept of tying together all the geospatial information." Remember that chart where I said we're going to bring

268

- **Command and control**
  - Connectivity between CINC/JTF/ component commanders
  - Connectivity among mobile tactical nets
  - Network management and control
  - Collaborative planning
  - Interactive video
  - Distributed database transfer
- **Integrated situational awareness**
  - Expanded battlespace picture
  - Imagery/SIGINT/HUMINT/MASINT
  - Timely weather information
  - Digital terrain maps
  - Support information
- **Support to shooter**
  - Specific system requirement
  - Real time essential
- **Analysis and training**
  - Planning
  - Training
  - Rehearsing

Figure 7

Warfighter Requires Expanded Information Capabilities

everything in to get us joint C⁴I for the Warrior better, cheaper, faster, and everybody would be able to communicate with each other (figure 5)? We rapidly found that we were building a Tower of Babel. The Air Force was building their own separate systems that use an Air Force common mapping system. The Navy has their own common mapping system, and your Army Chief of Staff, Gordon Sullivan, says that DMA is irrelevant. He needs digitization of the battlefield, virtual reality. "The Defense Mapping Agency isn't giving me what I need. I'm going to get my own system."

So, what have we got going on today? The growth of information systems is changing the geospatial information requirement (figure 8). We've got command and control systems that have to have a

3-D, digital WGS-84 (that's the Global Positioning System—GPS) coordinate database to operate against. We have weapons that can't get to the target without it. We have trainers that can't do without it; maps that can't do without it; models, simulations, and wargames (remember, I said I'm tying together my new 5105 and 4102, which come from wargaming, and then fighting in that real battlespace, and so it's got to be the same). We've got operating platforms, and they're all off on what Rosie calls the Tower of Babel, because they're all speaking different languages.

What we said to the Secretary of Defense is, "You need to go to a common set of geospatial reference databases, and you need to go there very rapidly. Time is of the essence. You are spending a lot of money building systems that we're going to have to scrap because they're not going to support the concepts of operation that General Shali and others have us all driving toward, and we're spending money on thinking we're going to get there."

That's how they went off and invented this second, parallel study, which I've given you a copy of (figure 9). "What the warrior needs: a fused, real-time true representation of the battlespace—an ability to order, respond, and coordinate horizontally and vertically to the degree necessary to prosecute his mission in that battlespace." Those words came out of the first study. I'm mixing things together. I don't want to confuse you, but this morass is careening down a railroad track, bouncing off the edges as we go.

Student: Sir, can I challenge you with something? The challenge is that the warfighters are the ones responsible for it, and let me take that step one little bit further. Goldwater-Nichols created these omnipotent CINCs out in the various areas, and each one of the CINCs has his own idea of what he wants over there. So, as opposed to beating us together into a joint thing where we can talk—not only services, but CINCs worldwide—each one of them has his idea of how he wants things, which is pulling us apart as opposed to pushing us together.
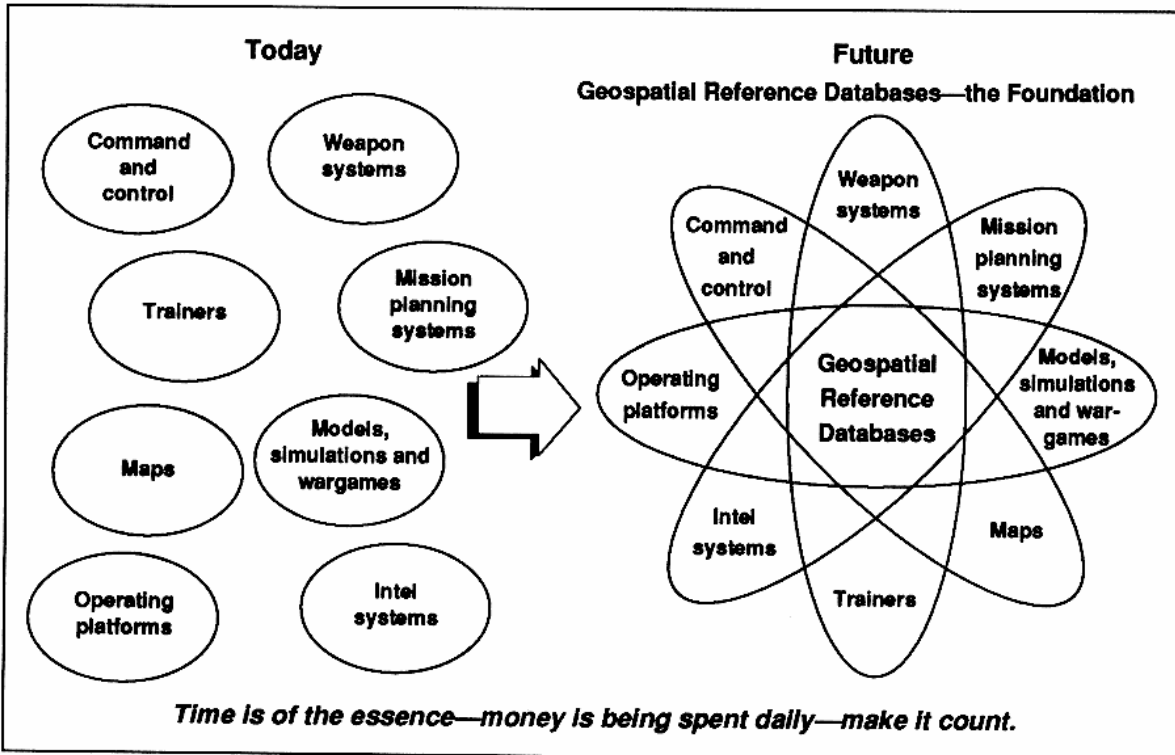
269

Figure 8

The Growth of Information Systems Is Changing the Geospatial Information Role

---

**Defense Science Board Task Force on Defense Mapping for
Future Operations, August 1995**

**G. Dean Clubb, Chairman
Major General Robert Rosenberg, Vice Chairman**

**"What the warrior needs: a fused, real time, true representation of the battlespace—an
ability to order, respond and coordinate horizontally and vertically to the degree necessary
to prosecute his mission in that battlespace."**

General John Shalikashvili,
CJCS—the C⁴I for the Warrior vision

Figure 9

DSB Mapping Task Force Mission

Rosenberg: You'll see that, but leaping ahead, that's why we are vesting the authority in the JROC to force commonality, because when the *Teddy Roosevelt* leaves, and the *George Washington* comes in, they've all got to be transparent, and they've all got to play to the same sheet of music. So we can't afford to let each CINC do it differently from the standpoint of his C⁴ISR building blocks. Now, we pay warriors to be independent and fight the way they fight. But the building blocks we want to give them—that is, the hardware, soft-

270

ware, information systems—we want to make common.

Student: Oh, I agree.

Rosenberg: Where that's getting resolved is that Bill Perry and Paul Kaminski and the Chairman of the Joint Chiefs of Staff are working together to insist that in fact we have common building blocks across the forces. Now, we're a long way from that. The world of reality is still those straight-ahead arrows (figure 5). I'm telling you the problem we face very realistically. It is: how do you positively incentivize our Air Force to build a command and control system that uses GCCS as the core operating environment instead of going off and doing their own thing?

Student: By the same token, the services need the same standardization. There was a big push separate from the unified commands, which are doing it for JROC, so that you could take a ship from the Pacific Fleet and transfer it to the Atlantic Fleet and there's no change in procedure.

Rosenberg: Heresy!

Student: But it took a while to get there.

Oettinger: Wait a minute, you took a while to get there. I think at one end of the scale, what you're saying is reasonable; at another, it's quixotic, it's unattainable. One of the reasons why the Tower of Babel myth is so pervasive and so long lasting is that it serves a purpose. What's wrong with the myth is that it suggests that we sinned and therefore it's a battle of tongues. It's not the case at all. Different tongues and different languages are optimized for different uses, and at some level, if you don't do that, you're in trouble. Now, there is some level at which what you're saying is true. I'm hoping that somewhere between now and when your briefing is done, you'll say something of where you think that breakpoint is.

Rosenberg: This is a vugraph that I put back in the book this morning when I was figuring out what I was going to show, be-
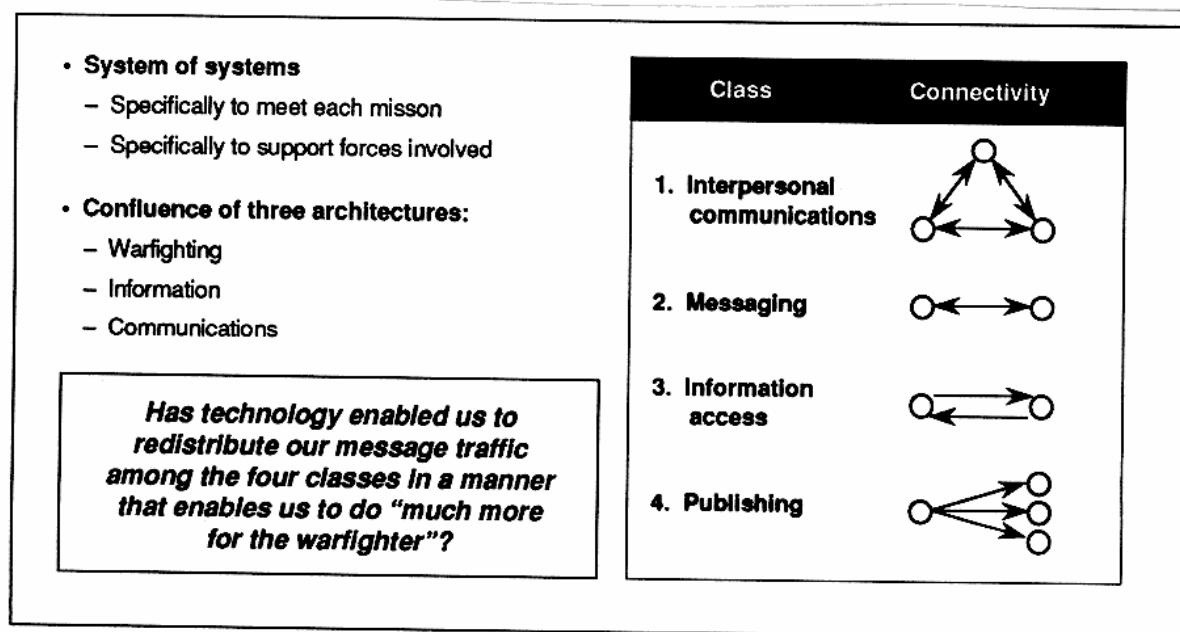
cause I thought we didn't have time to do this (figure 10). But you're off on a very important element of the concepts. Why you see *CINC's* warfighting architecture is that we're talking about a JTF as a system of systems specifically to meet each mission; that is, there is a reason not always to do the same thing. Remember, I said it's different every time. What we did was we codified three architectures: a warfighting architecture, an information architecture, and a communications architecture. Let me describe them.

In the commercial world, the analogy to the information architecture is building codes or standards. Building codes are constantly changing, and in the commercial IT marketplace, building codes are constantly changing. But these are the acceptable rules for interfacing things; they're the building blocks—how you put together the hardware, software, comm pipes, databases, and sensors to support the shooters. That has to be standardized. DISA is responsible in DOD for articulating those standards.
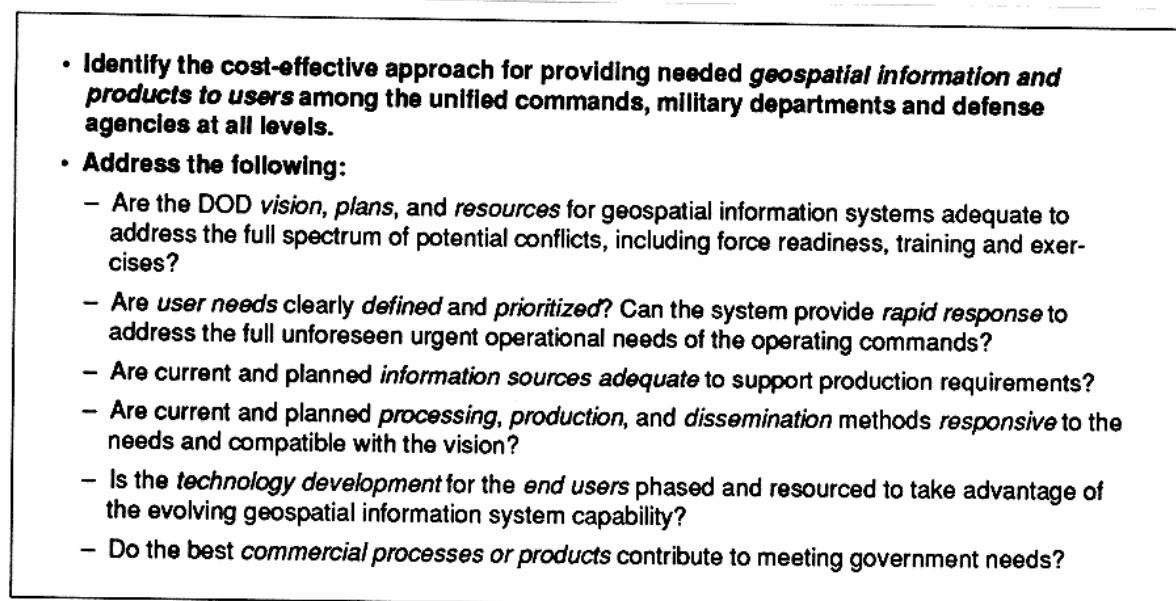
In the world of communications, the communications architecture—the Defense Information Infrastructure—provides a set of standards; there are standards in the way we do our communicating. The thing that is free play in these architectures is this: we're training you to be a two-star JTF commander some day, and we're training someone else to be a two-star JTF commander some day. There is no such thing as a cookie-cutter solution here. We're not going to build an architecture. You are going to free play like Fred Franks, Chuck Horner, and all the rest; free play, but using a better set of tools to do that than we have today.

As I said, while we were tripping along on the way, we tripped across the problem of all these different map bases, and, oh, by the way, today in Korea the maps that our Korean coalition partners are using are 700 meters different than ours are. That's what I'm talking about. I can just give you dozens and dozens of examples of that.

So we were asked to identify the cost-effective approaches for providing needed geospatial information and products to users (figure 11), and we were asked to look at, "Do we know where we're going?

Figure 10

CINC's Warfighting Architecture—Enables Battlefield Dominance

- **Identify the cost-effective approach for providing needed *geospatial information and products to users* among the unified commands, military departments and defense agencies at all levels.**
- **Address the following:**
  - Are the DOD *vision, plans*, and *resources* for geospatial information systems adequate to address the full spectrum of potential conflicts, including force readiness, training and exercises?
  - Are *user needs* clearly *defined* and *prioritized*? Can the system provide *rapid response* to address the full unforeseen urgent operational needs of the operating commands?
  - Are current and planned *information sources adequate* to support production requirements?
  - Are current and planned *processing, production*, and *dissemination* methods *responsive* to the needs and compatible with the vision?
  - Is the *technology development* for the *end users* phased and resourced to take advantage of the evolving geospatial information system capability?
  - Do the best *commercial processes or products* contribute to meeting government needs?

Figure 11

DSB Mapping Task Force Mission Terms of Reference

What do we want? Do the users know how to ask for what they want?" SOUTHCOM says they want 1:50,000 maps of all of Panama. What for? The mission is the defense of the Canal Zone. Did you know the last time a foot soldier slogged through 1:50,000 maps' worth of terrain in the jungle of Panama?

By the way, when I ran the Defense Mapping Agency, I did a study of where all those maps went. Those of you who have served in command posts: do you remem-

272

ber the two-story-high world maps DMA put out? I found one submarine in PACFLEET was ordering 90 percent of all of those. Where do they stick them all? When I was a lieutenant, I learned that having a dog-robber NCO was the smartest thing you could ever do, and there was a chief petty officer aboard this submarine who was getting these things and trading them for the best coffee makers and TV sets and microwave ovens and everything else. But the problem was, we weren't supporting the warriors. We weren't supporting Carl Stiner down there at the JSOC (Joint Special Operations Command) who needed to go in and pull U.S. citizens out in an emergency relief operation. So, our user needs had to be more clearly defined, prioritized, and associated with force readiness. Force readiness is how we should decide what our geospatial information should be.

So, with that as kind of a quick look there, now we're back to General Sullivan's digitization of the battlefield (figure 12). I'm trying to give you some vignettes of what's happening in the bigger picture of the DOD. General Sullivan said, "I must have virtual reality of the battlefield, and I don't have it today. We've got a lot of paper maps. That's not what we need."

I don't want to bother you with DOD buzzwords. In the world of digital mapping, we represent what the earth looks like by something called digital terrain elevation data (DTED), and what's important is how good is good enough. The Defense Science Board said, "It has to be something called

Level 2 or better. As a matter of fact, it needs to be about Level 50." You see, Level 1 is about as lousy as you can get, and Level 50 would kind of be like virtual reality. When I outbriefed Bill Owens (when he was the Vice Chairman, before he went to work for SAIC), I said, "Bill, I want to make sure you don't go to war anywhere except where I have this good virtual reality. Here's where we've got virtual reality. You can go to war with the Brits. (By the way, you could do it at our training ranges.) But, for God's sakes, don't go to war anywhere else in the world, because this is where we have a virtual reality kind of digital view of the world, nowhere else" (figure 13).

And why is that so?

Student: This might seem like a silly question, but why do you need this virtual map? I don't understand this. What can be gained from it?

Rosenberg: I didn't do a very good job of describing it to you. Let me give you just one repeat example. Every operation we go into is unknown. That is, we don't know where we're going to engage sniper fire. We don't know where that shoot-and-scoot artillery is coming out of those holes in the mountainsides in Bosnia. We don't know what's on the other side of the hill, so what we're trying to do, as our military operations people have to go into unknown contingencies—different places where they have not trained to be—is to provide them a sandbox to rehearse what they're going to

---

- **We have a lot of paper maps—this is no longer sufficient.**
- **At the minimum, Digital Terrain Elevation Data (DTED) Level 2 is required.**

Figure 12
The Digital Battlefield Requires Digital Terrain and Feature Data
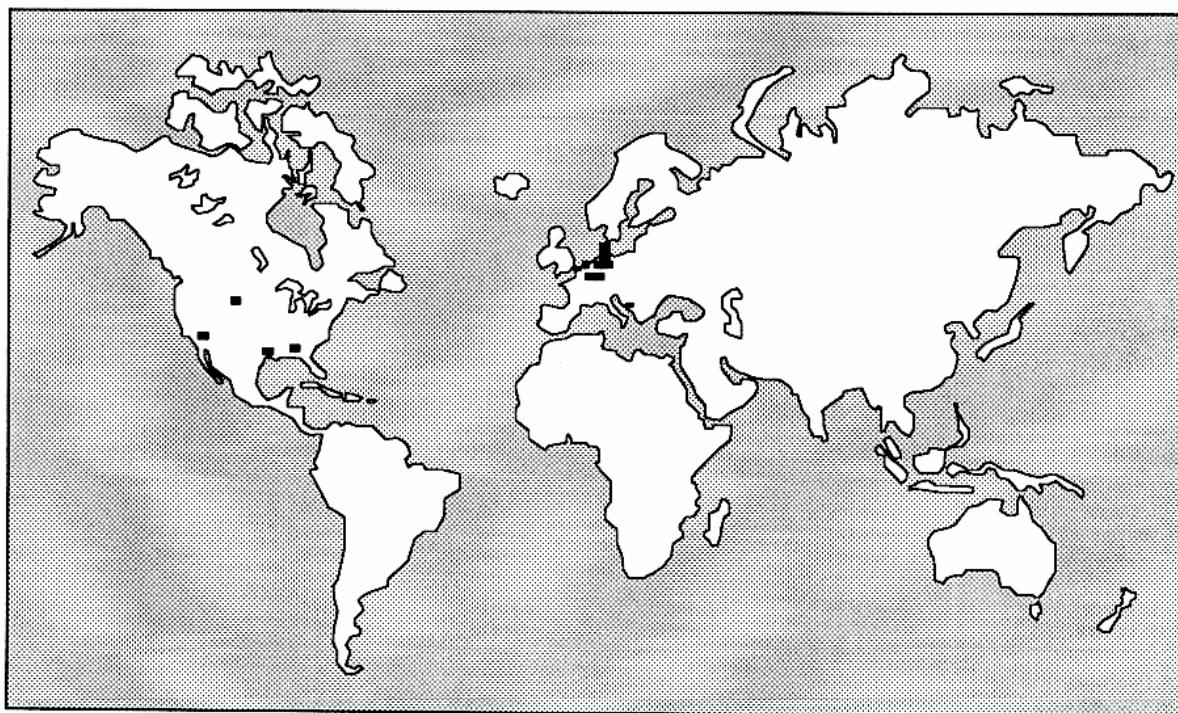
Figure 13

Digital Terrain Elevation Data Level 2 (DTED2) Available from DMA

get involved in before they get there, and it can't be very artificial.

Oettinger: And if you think that there are limits to this, think of the need for details about the interior of the airport at Entebbe.

Rosenberg: That's a very good point.

Oettinger: It isn't just terrain and things. Maybe at some point you want the inside of a closet, and the wiring diagram for the power supply of the airport at Entebbe.

Rosenberg: I take you back to the chart where I said, "When our political leaders see the risk of our people getting hurt being low, their propensity to want to play world policemen gets very high" (figure 4). Those who serve in uniform don't challenge their political leadership. They serve them, and the military tells them what they need to have to properly serve the political leadership who decide when they're going to use military force as a piece of national policy. You use the State Department negotiators. You use the Commerce Department. You

use all kinds of things short of a military presence. Bosnia is a good example where all those things didn't work until first we made a decision to bomb them in order to drive them to the peacekeeping table in Dayton. Then once they signed the peace agreement, we realized we had to put 20,000 U.S. and 40,000 coalition partner peacekeepers on the ground while they rebuilt and repaired and tried to establish stability in that region before we could leave.

Now, we can't safely put 20,000 people on the ground without doing a lot of rehearsing against all the contingencies that might happen there. That's why the ability to understand where I'm going is so important. It's this concept, which I went over too fast, of information dominance of the battlespace, when I used the chessboard analogy and I said, "I can see it all, I know it all, but unless I can rehearse getting killed many times before I actually have to go there, it's not safe for me to go there."

Student: I actually understood the necessity of simulations, given the lack of

274

operational experience. I guess I was confused by the terminology which you used: "We could only go to war in a place where we have these sorts of maps." I thought it wasn't necessarily the simulation that you were talking about, but rather, that there's this new standard of knowledge we need for any sort of operation we're talking about.

Rosenberg: You're catching that right. I come from a school where there's an interesting retired Marine four-star who, when the term "low-intensity conflict" was invented, said, "That's bullshit. When you're getting shot at, it's all war." So you'll have to forgive me for my outdated language. It's all war. Peacekeeping is a type of war in the generation I grew up in. I'm trying to keep the peace so I don't have to fight.

That's what most military people want: not ever to have to fight.

The problem we had was that the way we make those digital geospatial maps today is that we use satellite imagery from national reconnaissance satellites (figure 14). About 90 percent of all the imagery we use comes from those, and about 10 percent comes from commercial stuff. As a matter of fact, the U.S. Air Force can't plan missions and fly F-15s without using French imagery. That drives the Air Force mission support system. It's a crime that we are dependent, not on the French, but on one system. It's a crime that we are dependent for about 90 percent all of our mapping on imagery from one single source—national reconnaissance satellites.

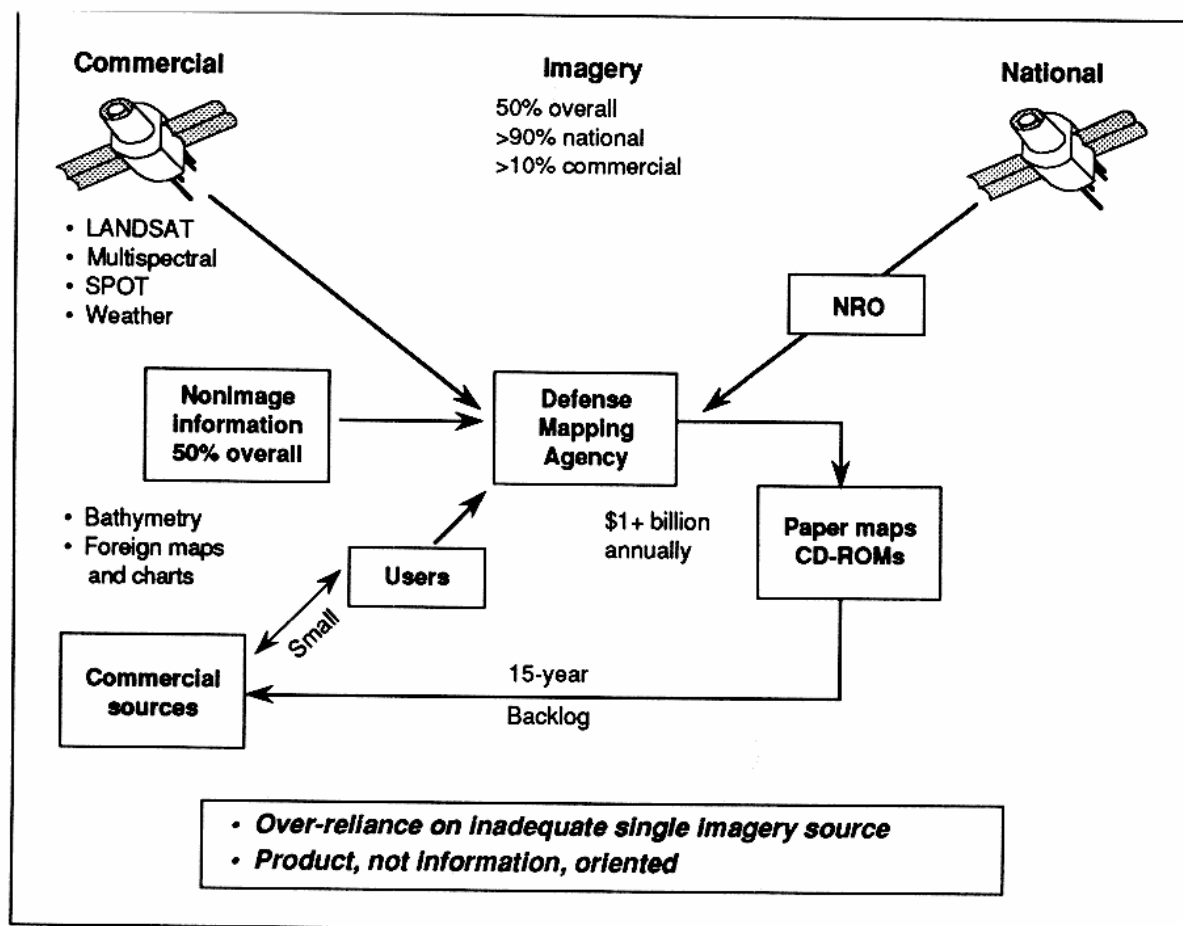The other half of the total input comes from bathymetry, foreign maps and charts,

Figure 14

Current Defense Mapping Process

and so on. We have a process where we spend somewhere over $1 billion a year with an outdated Neanderthal requirements process that creates a 15-year backlog. Any system that has a 15-year backlog is broken. So what's happening is that the warriors are going out to the commercial world and buying imagery directly from them, and buying commercial geospatial information capabilities from them, and enhancing the Tower of Babel. That's why, when forces deploy, land combat forces, air combat forces, and naval combat forces don't talk to each other, because they're all buying stuff from separate peddlers who are not working to any set of standards.

Now we're in the second study, and what we said is that the system isn't responsive (figure 15). The users, developers, and implementers are not closely linked together. We've got this stupid standard DOD seven-year acquisition cycle where we build stuff that comes seven years after it's useful. Our coverage requirements process isn't effective. We have fielded weapons systems that have no digital brains to fly them. Security issues limit dissemination of products: they're overclassified.

We thought all that could be fixed, so we established a vision. Let me take a minute to explain this vision to you, because it's central to where DOD is now going, where they're spending money, and this has been approved at the SECDEF and DCI

levels. The concept is that for all military information systems, we need a common geospatial reference database (figure 16). What do I mean by that? Its baseline is imagery, terrain, and bathymetry that is very accurately located—GPS accuracy location and better. Then it's all time tagged, and it's all pedigree tagged so that ...

Oettinger: "Time tagged" meaning the time at which that information was valid, so you know it was taken five minutes or five years ago? Is that right?

Rosenberg: As a matter of fact, in distributed digital databases, the modern commercial information systems allow you to have several different pieces of data with the same location but different time tags. For example, a CINC's land combat forces really don't want useless tactical terrain data on the wintertime if it's summertime. They want to know go/no-go conditions for main battle tanks and for armored combat vehicles. They want to know it tomorrow when we move, so they want to overlay today's weather for today's combat operation and tomorrow's weather forecast, geospatially gridded and time tagged over that battlespace, so that the commander can mission plan tomorrow for what's going to happen. Then he can decide, "Can I use EO (electro-optical) weapons, IR (infrared) weapons, or radar weapons?" depending

---

> - **The DOD system isn't responsive to 21st century needs.**
>   - Users/developers/implementers not closely linked
>   - User geographic coverage requirements process is ineffective.
>   - Weapon system requirements have not always been included.
>   - Security issues limit dissemination of DMA imagery products derived from NRO sources.
>   - Long production pipeline causes excessive backlog. Feature extraction is a major contributor.
>   - Minimal production standardization
>   - DOD is making major investments in modernizing military information systems without a common interoperable geospatial foundation.
>   - There is not a single DOD coherent vision of the future—in fact, there are many separate visions.
>
> *These problems can be corrected within current budget projections.*
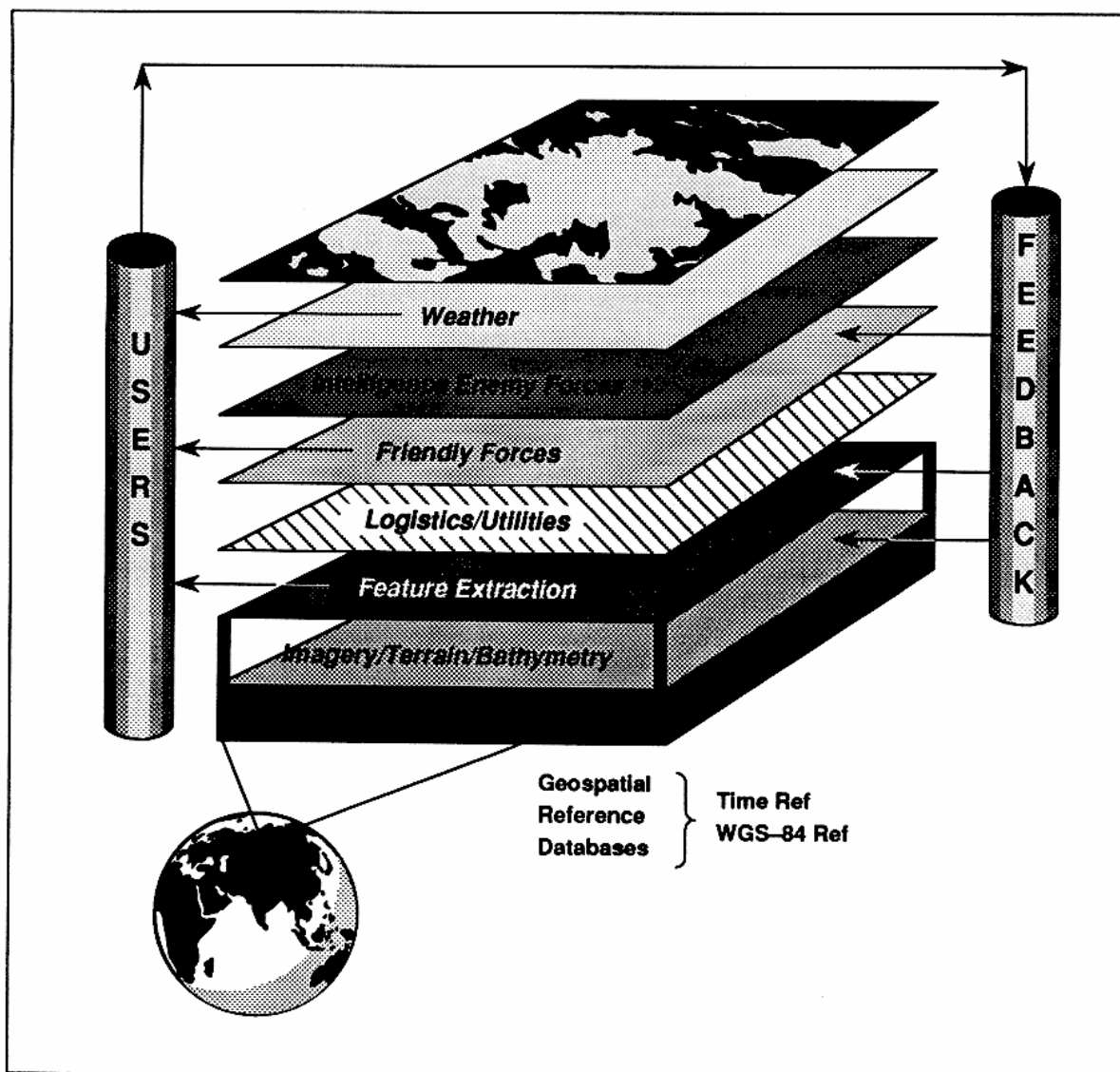
Figure 15

Findings

Figure 16
Our Vision: A Time-Tagged Geospatial Foundation

on what the battlespace conditions are. So the concept is to have these features, to have underground utilities so I know where the hell to cut the integrated air defense system cable: friendly force information, bad-guy information, neutral ... the entire battlespace—blue, gray, red. Like that 14-year-old sitting at home on the PC, users should be able to pull out of different levels of these databases the information that they need to build their customized products to support their mission needs, and, oh, by the way, to provide feedback.

An example: I am sitting out there on the hillside, and I am a forward air con-

troller, and I've got to vector in attack helicopters or A-10s to do a strike against terrorist artillery in Bosnia that has come out. I look at my Hum-Vee soft-copy display, and I see a digital, three-dimensional picture of the valley. I look out there, and there are power lines across there. My A-10s and my attack helicopters are going to fly into those. I should be able to feed back into those databases what the world looks like right now so that they don't fly into them. When I do battle damage assessment, I must change what the world looks like on my maps. For those of you from the military, the concept is to fuse

277

together the world of the J-2, the J-3, and the J-6, instead of having each building their own separate databases.

The Defense Science Board felt the key to making that happen was commercial leadership, since commercial sources are the primary suppliers of fused, spatial-related data services and products (figure 17). We're spending $1 trillion a year. That's far more than we're spending in DOD. Commercially available imagery is becoming available: IFSAR (intermediate frequency synthetic aperture radar) and SAR, commercial global broadband communication systems. Our advice to the Secretary of Defense and the defense leadership was, "You'd better take advantage of what's going on out here. Your enemies are already taking advantage of it."

Student: How do you mean that, sir? I'd say we're a generation or two ahead of everybody else, and our challenge is just to stay there and advance further.

Rosenberg: Are you a student of Toffler?

Student: Well, I've certainly read Alvin and Heidi's four or five books, so, you know ...

Rosenberg: There's a chapter on this that we probably won't get to. But in the world of information warfare, I can assure you that a level-2 nation can bring a level-3 nation down to its knees in information warfare. The point is that while we may have very, very sophisticated reconnaissance systems, and information systems, and surveillance systems, and battlefield information flow, a much less sophisticated adversary who can take advantage of tactics, terrain, and information—as they did to us in Vietnam, as they've done to us in other places—can certainly bring us to our knees. No, we're not that much better, not unless we know how to use the tools better.

Student: That may be true. It's very opaque how a given nation, culture, or organization is able to use technology. The technologies they can buy are pretty clear. But whether they can turn that into organizational effectiveness is very hard to measure.

Rosenberg: Absolutely. It's hard to measure, and that's why we have to be prepared. I don't want the message to escape you. Look at the date up there. You're talking today; I'm talking about what is out there on the horizon. You've heard Admiral Owens talk about what if the Chinese decide to spend 6 percent of their GNP on military capability instead of 1-1/2 percent of their GNP? They can afford to buy all

---

- **Commercial sources—the primary supplier of geospatial-related data, services and products by the year 2000.**

  - The global information infrastructure *investment* exceeds $1 trillion per year. High *leverage* for supporting future geospatial architecture.

  - Commercially available *imagery* of 1-meter (panchromatic) and 4-meter (multispectral) resolution will be *ubiquitous.*

  - *Commercially available* digital terrain data derived from aircraft and orbiting SAR, IFSAR and imagery platforms will be the *major source* for the global geospatial databases.

  - Commercial *global broadband communications* developers are implementing *robust, secure, high-capacity* terrestrial and satellite networks which will exceed DOD capabilities.

  - *Commercial* markets are driving geospatial *standards.*

 *DOD: Take advantage of commercial world—others will!*

Figure 17

The 21st Century: Commercial Leadership

278

this capability. So can other nations, because it's not the private domain of the United States. The point is that these kinds of capabilities, which far exceed our current fielded capability in the Department of Defense, can be bought off the same "Safeway grocery shelves" on the international marketplace by all our adversaries where we can buy them.

For those of you who weren't there, I told the small group that had lunch with me that every time I went to Rome Air Development Center, the Air Force's information technology laboratory, the colonel used to show a chart that said, "My job is to transfer U.S. military technology to the commercial world." I said, "You know, I'm going to shoot you if I see that chart again, because U.S. Air Force C^{4}I technology is

behind where the commercial world is. So don't tell me your job is to transfer it out. Your job is to provide the unique military value-added research and development to take advantage of what's out in the commercial world better than our adversaries."

So, what we said was, "In that future process, we should take advantage of everything that's out there" (figure 18). By the way, this has nothing to do with mapping. This has to do with moving digits of information around the battlespace. We should take advantage of everything, including our own operators, including what's going on in the commercial world and the international world, so that the Air Force is not dependent on just SPOT Images. When we go to war with a French
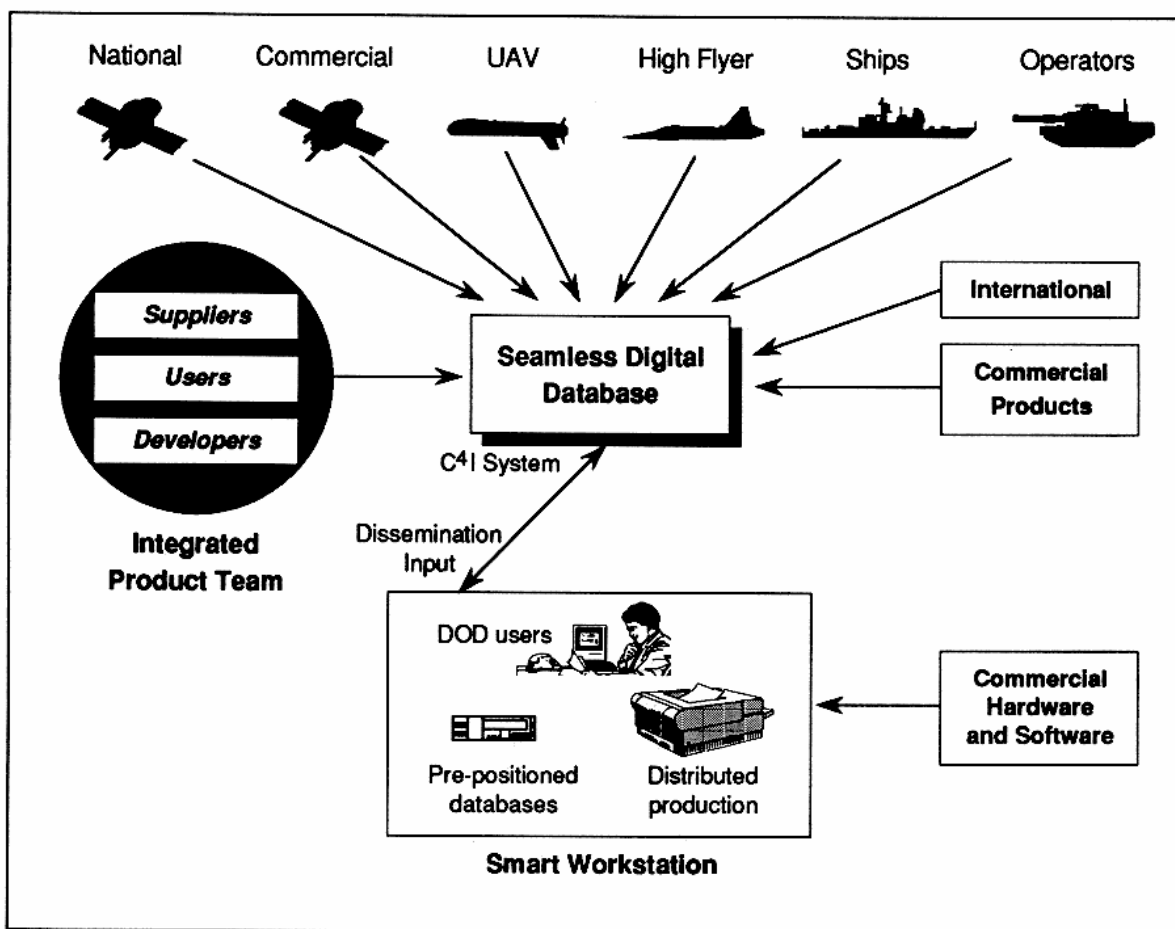
UAV = Unmanned aerial vehicle

Figure 18

Future Defense Mapping Process That Meets Our Vision: What is DOD's Vision?

279

ally, and they turn that off, I want to be able to use Japanese imagery, Russian imagery, American imagery. It should be fail soft. It shouldn't be dependent on a single source, just as I don't want to be dependent on the national reconnaissance program, and I want to be able to provide that ability to DOD users through seamless digital databases, using pre-positioned databases, smart workstations, and their own distributed production to satisfy their needs.

What we want to be able to do in the operational implementation of that vision is pull in all kinds of information from the commercial world, not just using the Defense Information Infrastructure, but through appropriate gateways with firewalls and guards (figure 19). We need to pull in all kinds of information through the Internet from the commercial world to support our military operations. There is a vast amount of information out there that we are not using wisely today because we don't take advantage of what's there, and we need to do that.

Now I'm back to study number one (figure 20). What we said was that we want to be able to empower that Joint Task Force commander at all levels to be able to control the information he needs to execute his mission. This goes back to a much earlier conversation about flexibility. These are the stovepipe systems I built when I was on active duty, where the general has all the information and the poor shooter has nothing. This doesn't mean we want to saturate the shooter with information, but the comm pipe capability and the digital database
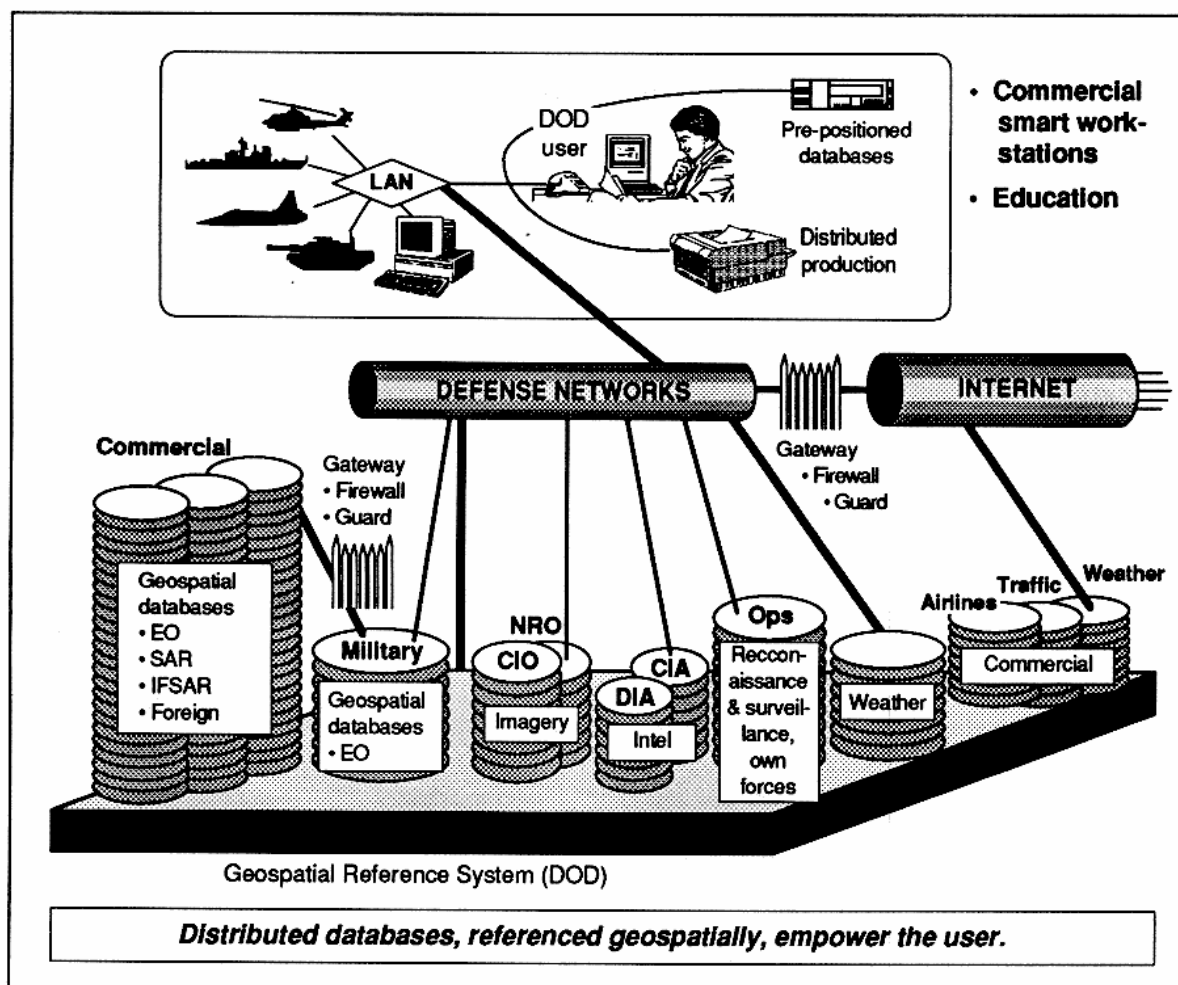

Geospatial Reference System (DOD)

Distributed databases, referenced geospatially, empower the user.

Figure 19

Vision—Operational Implementation

capability are there to provide the information at this concept level. You can think of every one of these kind of as a rheostat that I control. I come to the ballgame and say, "Here are all the essential elements of information I have. Here's the frequency by which I need them, the timeliness, the fidelity, the resolution, et cetera, and I pull what I need in combination with a military CNN capability."

Oettinger: Let me just ask about that, because what I see here is the Tower of Babel reasserting itself, and therefore the need for training and practice. It seems to me that those two go hand in hand. The point of the training, presumably, is to familiarize someone with something, which at this level is never going to be standardized.

Rosenberg: Absolutely. But you see, that's the tie-in with the world of modeling, simulation, and wargaming. If it's seamless

between that and real operations, then you get your training in the environment you're really going to operate in. So when you plug and play in the simulation world, it's the same plug and play you're going to operate with.

How do we get there? Well, every other nation in the world, and what's going on in the commercial world, everybody is taking advantage of direct broadcast except us (figure 21). You can look all over the world and see 18-inch pizza pie antennas out there with people receiving information directly.

Student: Where, sir?

Rosenberg: I will send you some documentation: Indonesia, India, China ... everywhere.

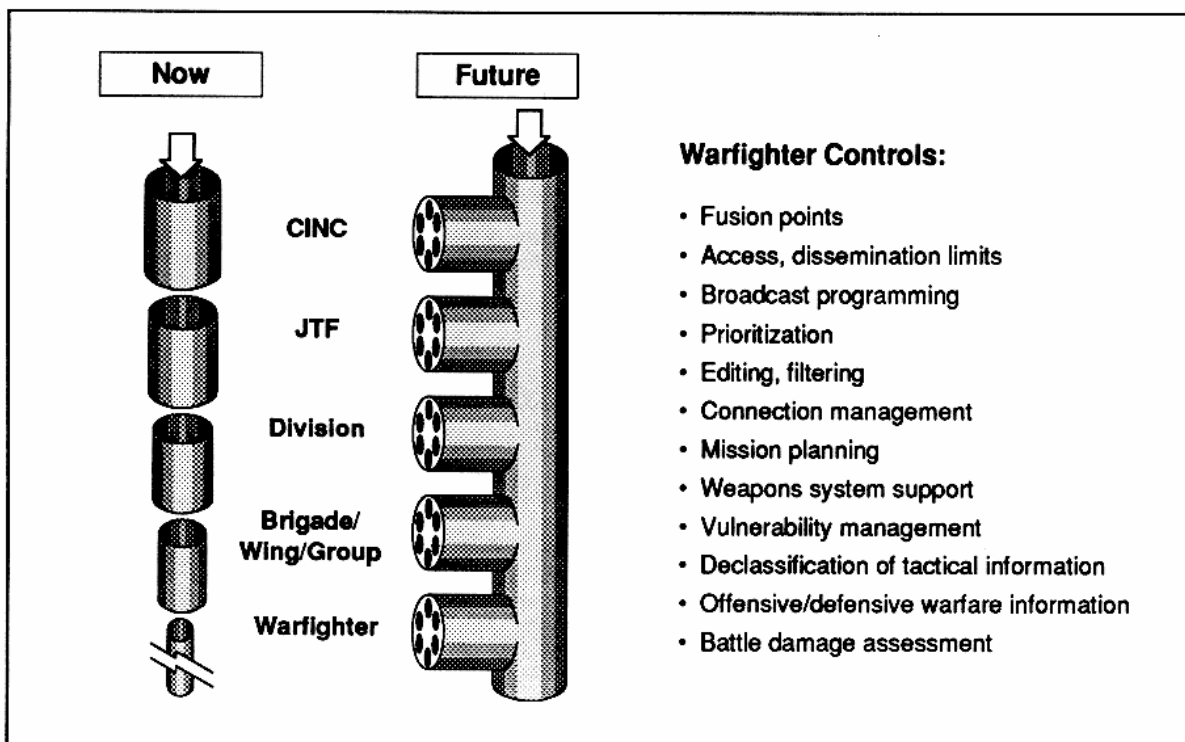**Student:** When you go to Taiwan, there's a broadcast dish on every house.

Figure 20

Empower the CINC to Fashion His Own Information Processing and Delivery System

Oettinger: The entertainment satellites have broadcast to 18-inch dishes all over the place.

Student: Were the militaries using that?

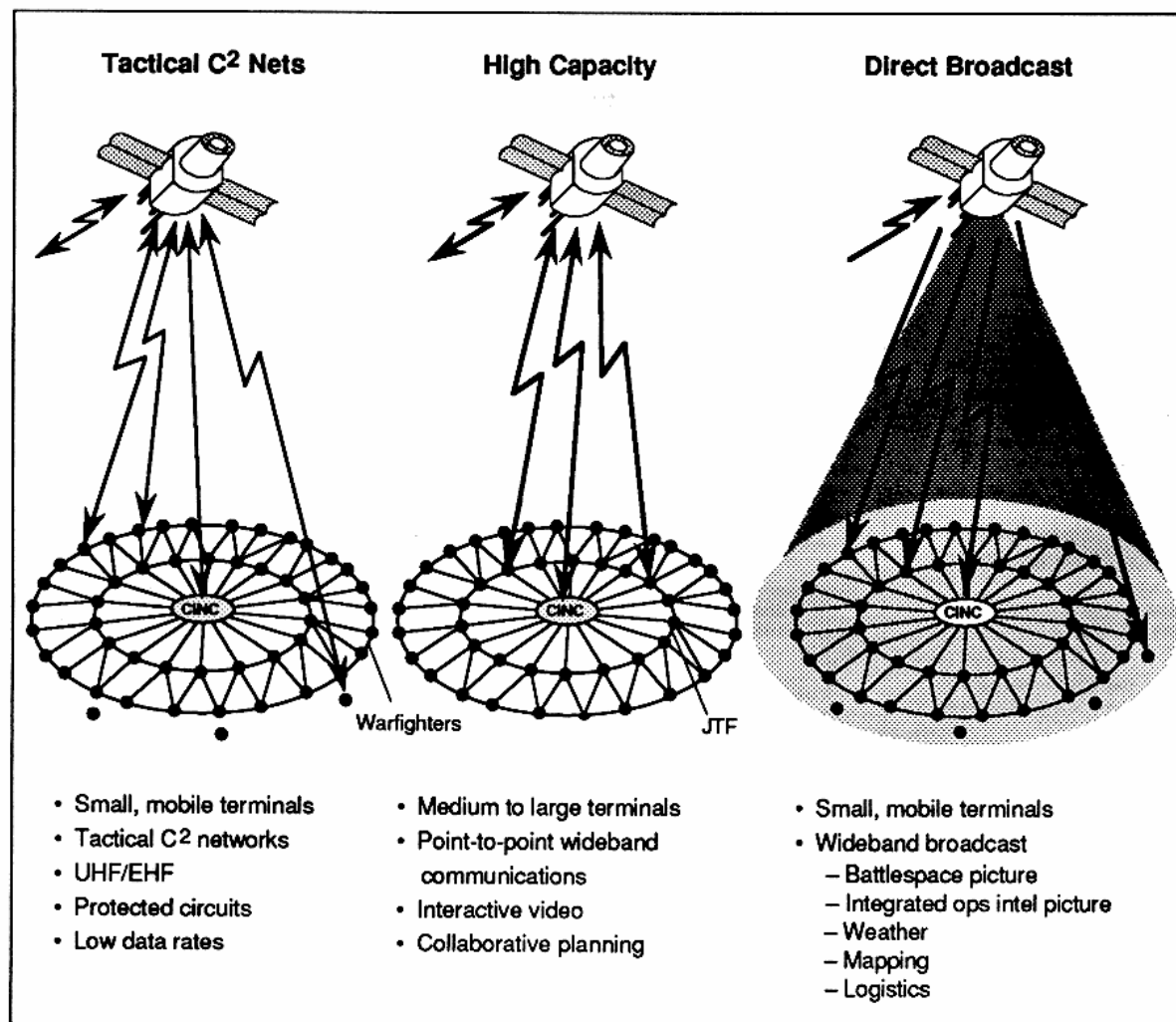**Student:** No, that's the point.

Rosenberg: You're missing the point. Let me tell you ...

Student: Well, tell me, sir, because I really want to learn it.

Rosenberg: That's where I'm headed. Given the ability to provide all these large digital distributed databases, we need the capability to have wideband communica-

tions to pump that information around, which means our dependency on outdated MILSATCOM designs—things like Milstar that were built for nuclear warfare, things like DSCS (Defense Satellite Communication System) that aren't responsive to the needs of our operational military forces today—goes away or changes. The solution is for us to use the wideband commercial communications capability and the fiber optic networks that are virtually enveloping the world today. When I was over in the Bosnia campaign, we were not tied in to the Italian fiber optic system. That's criminal! We should have been pumping wideband data all over Italy through that wideband fiber optic system.

The point I'm getting to is we want to

Tactical C² Nets

High Capacity

Direct Broadcast

- Small, mobile terminals
- Tactical C² networks
- UHF/EHF
- Protected circuits
- Low data rates

- Medium to large terminals
- Point-to-point wideband communications
- Interactive video
- Collaborative planning

- Small, mobile terminals
- Wideband broadcast
  - Battlespace picture
  - Integrated ops intel picture
  - Weather
  - Mapping
  - Logistics

Figure 21

The Future

282

use wideband commercial capability to provide battlespace pictures, integrated ops, intel pictures, and weather to small mobile terminals. I want to be able to turn the channel to 20.2 if I'm a battalion commander, going back to the last chart, and get the situation awareness environment covering my battlespace the way I call for it to be tailored. If I'm an F-111 wing commander, I want it a different way and I go to channel 20.5. We are, in fact, fielding a prototype over in the Bosnia theater today of a broadcast management system in the Bosnia theater doing the kinds of things I'm talking about.

Today DSCS is choked up. We're going to offload all those gigabits of data onto the systems that can easily handle them, so that we can use systems like DSCS to do what I told you before was critical and we can't do: collaborative interactive planning among the land, naval, and air components—interactive, video collaborative planning. Systems like DSCS can do that. We can transfer Milstar, EHF kinds of systems, from nuclear warfighting machines to something useful in today's operations other than war world, which is tactical command and control nets, to users who, in fact, can only have low data rates, and who don't have the capability for more.

Student: I don't question at all what you said on this slide. I absolutely agree with it. I just think that we are pushing the envelope, and want us to continue to do so, and the suggestion that others are ahead of us or challenging us here I find hard to believe.

Rosenberg: I didn't say others were ahead of us. You misunderstood. The chart said, "21st century" (figure 17). The chart said that this commercial capability is out there. It is not the private domain of the United States Department of Defense, and others who choose to use it, if they use it more efficiently and effectively than we do, can, in fact, dominate the battlespace

When I went over to the Bosnia theater, when Secretary Perry sent us over there, the Bosnian Serbs had information dominance of the battlespace there.

Student: They could have ...

Rosenberg: They did have. They were inside our cycle time. They determined when and where events were going to take place. Now, there were a lot of reasons for that. Our OPSEC (operational security) was abominable. Our COMSEC (communications security) was abominable. There were a lot of reasons, but the excuses don't matter. The point is that an outfit against whom we consider ourselves giants was controlling the operation. That's all changed now that we're in an operational military environment.

Oettinger: Measures and countermeasures don't stop. As someone said at lunch, the technology doesn't stop. I was moved to this remark by thinking back to General Lee Paschall coming here years ago to this seminar.* He was grateful for a bit of DSCS connectivity, and now we're hearing you say that DSCS is a choked-up thing. Expectations rise along with the technologies, and quite aside from what they could do to us, there is also the question of what our own expectations are.

Rosenberg: Yes, and remember, what we're trying to do is use what the technology will allow us to use in order to make this concept of information dominance of the battlespace work for us. That's where this all comes from.

This is a chart I wish I had put up a long time ago, and I'm only going to talk to a couple of the recommendations we made (figure 22). One of the things we said is that the only way you're ever going to get there is to put a "sandbox" out there—a place where the warriors can have some tools to play with to try these things. (The "sandbox" is a Fort Leavenworth term, long before you went to school. Now they use computers, but back when I was there, they had a sandbox.) In the world of C4ISR, remember I said I want to be able

---

* Lee Paschall, "C3I and the National Military Command System," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1980.* Cambridge, MA: Program on Information Resources Policy, Harvard University, December 1980.

Figure 22

Create Battlefield Information Task Force: An Instrument of Change

to plug together hardware, software, comm pipes, databases, and sensors to support the shooters. You have been in this course for a year. Do you think there are any metrics at all on whether plugging together A, B, C, D is any better than E, F, G, H? What we said was we need to have a thing where we bring together warriors and developers to establish the future vision, system needs, and evolutionary development plans; create and use joint battlespace modeling and simulation for requirement trades, training, exercises; and develop ACTDs to optimize existing capabilities and demonstrate future growth. Let's go out and try this military CNN thing. Let's do an experiment and see what is useful and what is not useful. Let's get away from this stodgy, seven-year acquisition process that doesn't let us find solutions to the C^4ISR support problems to our warriors. We need to exploit current science- and technology-based programs, demonstrate combat potential of C^4I improvements, identify and track performance metrics (I just talked to that), and provide recommendations to developers. I'll talk about this Enterprise

Integration Council, which is the JROC JWCA on C^4ISR that came out of that recommendation.

We said, "Set this up." During the course, I'm sure you've become aware of things like the Battlefield Awareness Data Dissemination (BADD) and Advanced Concept Technology Demonstration (ACTD) that ARPA/DARPA is leading. There's also the Bosnia ACTD, which is providing a warrior sandbox over in the Bosnia theater. We're doing the same thing with the joint precision strike demonstration over in Korea. The threat over there is a 240 MLRS (multiple launch rocket system) and 170 MLRS threat that comes out of the tunnels and is a rain of terror at Seoul. It's the political threat, just as the Scuds were against Israel. Those are all examples that have come out of this concept. I'm giving you some real examples of where we are spending money now in DOD to implement this concept of this battlefield information task force, which addresses a lot of issues we've been debating. We did not have answers to, "How do you train for this?"

I talked to this chart earlier (figure 23). Do you remember when I used the vignette where I said that when we put a piece of command and control capability up at the PRISM Rapid Prototype Center, milliseconds later we want to do a virtual reality wargame in Korea? What the world of the Defense Science Board says we should

- **Combine and expand our capabilities for exercises, games, simulations and models**
  - From the same seat
  - For:
    - Readiness assessment
    - Requirements for acquisition
    - Debugging
    - Verification of interoperability
    - Training
    - Rehearsal
    - Confidence building
    - Mission planning
    - Battle damage assessment

  Action: DDR&E (DMSO) with USACOM, JWFC and J-7

DMSO = Defense Modeling and Simulation Office
JWFC = Joint Warfighting Center

Figure 23

Virtual Conflict Every Day

move to, and Anita Jones,* and Paul Kaminski, and the SECDEF, and Bill Owens all agree and are spending money to get there, is back to Rosie's vignette, and that is your 15-year-old kid sitting at home, surfing cyberspace. We want that warrior sitting at his operational workstation, using the world of modern, commercial information technology tools and capability for readiness assessment, requirements for acquisition, debugging, verification, interoperability, training and rehearsing, confidence building, and mission planning, and doing everything virtually from the same

seat. The message was: we don't need big acquisition communities in this new world separated from the real user. We need them working much more closely together.

Let me go very rapidly through the rest of the briefing so we can have time for a couple of questions at the end.

Oettinger: But you've been getting questions all along.

Rosenberg: Yes, but I want to get to the end. I want to talk quickly about the information warfare threat (figure 24). I'm going to skip over it fast by saying the threat is serious. A large structured attack with strategic intent against the United States could be prepared and exercised under the guise of unstructured activities. This is directed at your comment to me earlier, when I talked about Toffler. I can't go into any further detail at an unclassified level than this: we had a major year-long Joint Security Commission study that produced an unclassified publication that you should get up here at Harvard. It was done about two years ago. It was co-chartered by the Deputy SECDEF and the DCI, and it was of major concern.

- **Structures**
  - Over 100 nations with capability
    - More than 50 target the U.S.
    - Some have computer intelligence efforts
  - Transnational, multinational corporations, terrorists
- **Unstructured**
  - 25 countries with computer underground groups
  - International hackers
  - Individual hackers very sophisticated
- **Really a continuum**

  A large structured attack with strategic intent against the U.S. could be prepared and exercised under the guise of unstructured activities.

Figure 24

Threat

---

* Anita K. Jones, Director, Research and Engineering (DDR&E), OSD.

Why is it of major concern? Because our global information infrastructure that supports military operations consists of all these kinds of things that don't have, in many cases, any protection from meddling by outsiders (figure 25). Information warfare is not me zapping your information systems and you zapping my information systems (figure 26). Information warfare is all of these things—INFOSEC, espionage, information influence, electronic warfare, destruction, perception management, and deception. Remember, I talked earlier about the example of speed and screwing up somebody else's image of the battlefield if necessary. All those things need to be taken into account.

Quickly looking at the technology base, this is just another way of saying to you what I've said many times (figure 27). This is the Fort Leavenworth sandbox. We and our adversaries can buy all the same stuff from the same commercial world, essentially the same commercial information systems. He who glues it together with the best unique military value-added investment is the one who, in fact, is going to have information dominance of the battlespace.
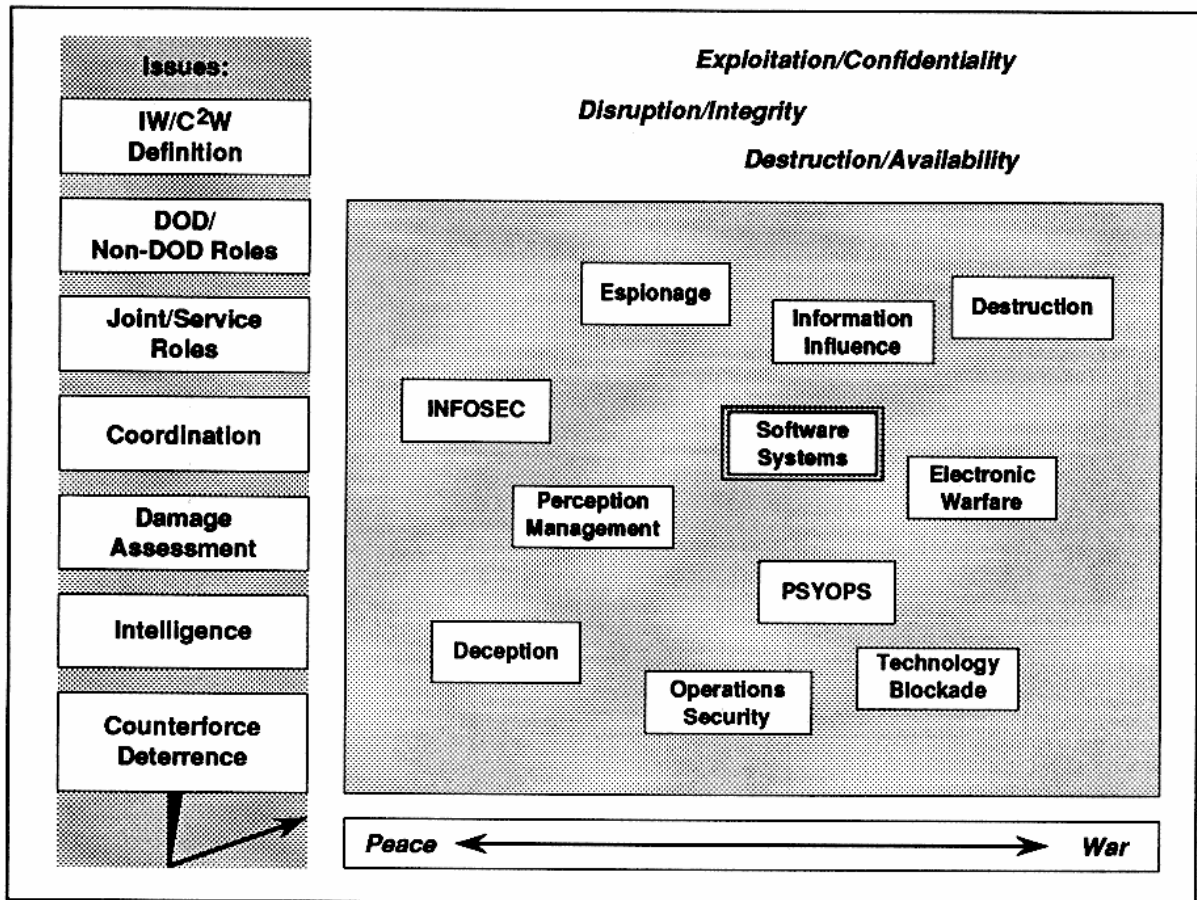
In the DSB study I gave you, there is a major section that talks to architecture and technology, and these charts just summarize it at a very top level (figure 28). It says here, "For that enhanced kludgeability—gluing hardware, software databases, comm pipes and sensors together—the third column (Information Movement) is for the movement of bits and bytes, the second (Information Assimilation) is how to put it all together, and the first (Joint Battlespace Environment) is plugging all that together. Where there is an open box, it means: 'Take advantage of what the Bill Gateses of the world are doing. Stop wasting DOD money trying to invent new things because the commercial world is ahead of you.' Where there are stars, it means: 'In these areas, the commercial world is not spending the money. In order to have this enhanced kludgeability, or enhanced reconfigurability, we in the Defense Department need to be the leaders for those kind of things.'"

A similar chart was built for the information warfare side of the house—information and information systems protection (figure 29)—and you'll notice a lot more

- **Media and Infrastructure**
  - U.S. public switched networks
  - Commercial communications satellite systems—U.S. and foreign
    - Intelsat, Inmarsat, Panamsat
  - Navigation systems
  - Transoceanic cable systems
  - Global Positioning System
  - Foreign telephone and telegraph
  - Databases
  - Internet
  - DOD MILSATCOM
    - Milstar, DSCS, UHF
  - Tactical networks and C^2
  - Supporting infrastructure
    - Power grid, commercial system support, spares, maintenance, transport, etc.

Figure 25

Global Information Infrastructure Supports Military Operations

286

Figure 26

Information Warfare

Within the figure, the following labels appear:

Issues:
- IW/C²W Definition
- DOD/ Non-DOD Roles
- Joint/Service Roles
- Coordination
- Damage Assessment
- Intelligence
- Counterforce Deterrence

Exploitation/Confidentiality
Disruption/Integrity
Destruction/Availability

Espionage · Information Influence · Destruction · INFOSEC · Software Systems · Electronic Warfare · Perception Management · PSYOPS · Deception · Operations Security · Technology Blockade

Peace ← → War

PSYOPS = Psychological Operations

stars. In a simple word I'll tell you that you pay for that on your Visa card, because in the financial world, the banking world, SAIC has many, many clients. We're in the commercial information systems protection business. We don't hear from these folks until $400 million disappears from the databases; then they call in the SAIC firefighters to put in the gates and firewalls. But information warfare protection is an area where we need to make some significant investments.

So we concluded that technology is not an impediment to information dominance of the battlespace, and that the commercial information industry leads in that area (figure 30). It's available to bad guys as well as good guys, so we should invest in military-unique information technology R&D. Those two vugraphs, of which there are about 40 pages in the document I men-

tioned earlier, are the cited guidance in DOD as far as incremental funding approval on what kind of money should go into the world of C⁴ISR R&D investments.

Quickly looking at business practices, you heard me say about a dozen times: "The JROC JWCA, C⁴ISR is how we're solving this." This kind of messy, gobbledygook chart out of the study says that there are things called the Enterprise Integration Board, the Enterprise Integration Council, and the Warfighter Information Requirements Architecture Framework (figure 31). Remember, I said there were three architectures: information architecture, communications architecture, and warrior architecture. The Council was only working the first two—information architecture and communications architecture. In other words, we technocrats—ASD C³I, the SCs of the world, the communications
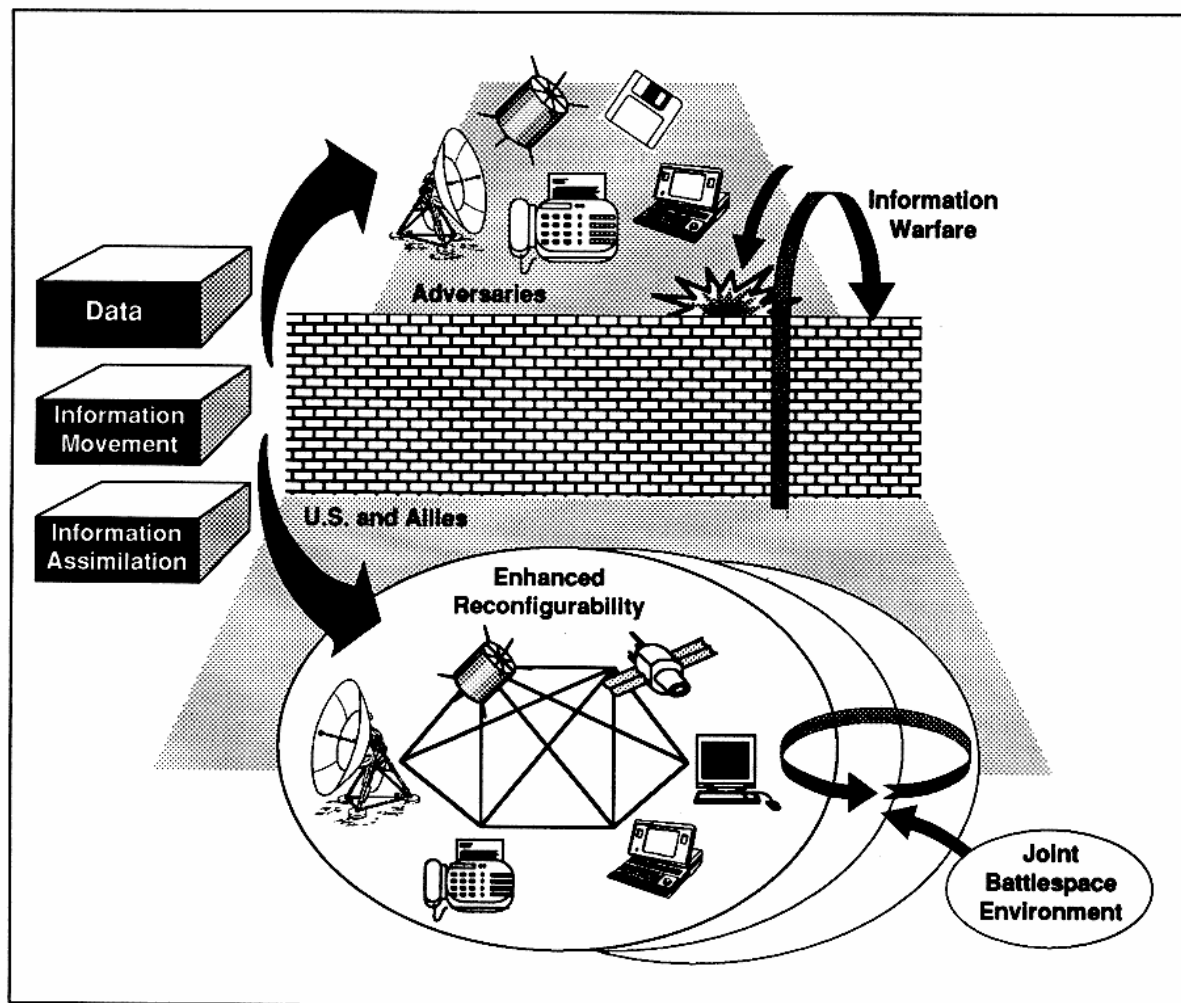
287

Figure 27

R&D for Information Dominance: Information *in* Warfare/Information Warfare

commands, and the information systems commands—were all working together, but the warriors weren't driving it. What we said was: "Take this whole process of the sandboxes—USACOM has one, Korea has one, we're building one over at EUCOM—and let them begin to experiment with how they can take advantage of C⁴ISR as a more effective force multiplier." You remember a chart way back when that said, "Part of our problem is that the joint warrior isn't smart enough to know how to ask for what he needs" (figure 6). This whole process has enabled Admiral Owens, and now General

Ralston,* to begin to get their hands around investment decisions on where to put our money on future C⁴ISR capability.

I've already briefed you on this chart (figure 32), but I'd recommend you read this portion of the document. This is where we admonished the leadership and said, "We really like what you're doing on acquisition reform on the 5-to-50-year life-cycle systems, but that bears no relationship to where the real serious problem is, and that is taking advantage of what's going on here in this world."


* Gen. Joseph W. Ralston, USAF, VCJCS, 1996 –.

288
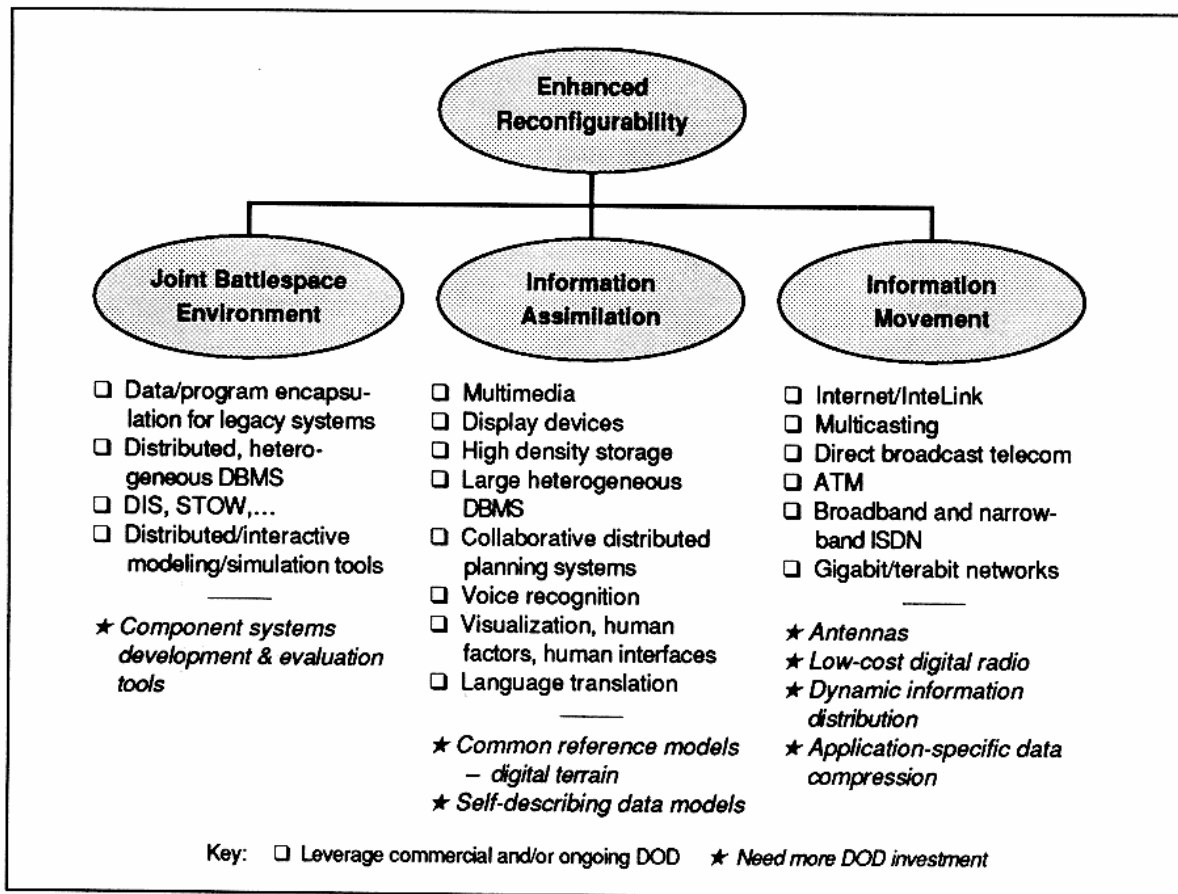
Figure 28
Architecture and Technology – 1

There are a few stories that I told people before the class was assembled, and one of the stories I think is worth repeating. I have a very highly classified customer to whom I took a briefing about a year ago on how to migrate out of large, stovepiped custom information systems into the modern world of the open system. At the end of my presentation, the senior officer said, "Rosie, why is it that none of my contractors ever told me stuff like this?" I said, "Well, it's because they lived behind the same compartmented security door that you and all your people live behind. You don't know what's going on out in this world. You keep on building and maintaining these large, expensive systems because you really are out of touch with what's happening in that real world out there." I suggested to this senior guy that if he called in all of his big systems contractors and said, "Give me a briefing on how to take advantage of modern commercial information systems, and if anybody comes into the room with a special security clearance, I'll cancel my contracts with you," I said, "I'm sure you'll get the same briefing I gave you, because the IBMs, the Lorals, the Hugheses, all these companies are doing this. They're trying to take advantage of the major investments that the Bill Gateses of the world are making."

This is a summary of the recommendations out of those last two charts I showed you (figure 33). This was the recommendation to establish the sandbox ACTDs, which are all being fielded now, and to modify the JROC process and charge the Vice Chairman of the Joint Chiefs of Staff with treating C4ISR just like we treat weapons, and that is, as being just as important to the capability as adding weapons.

289
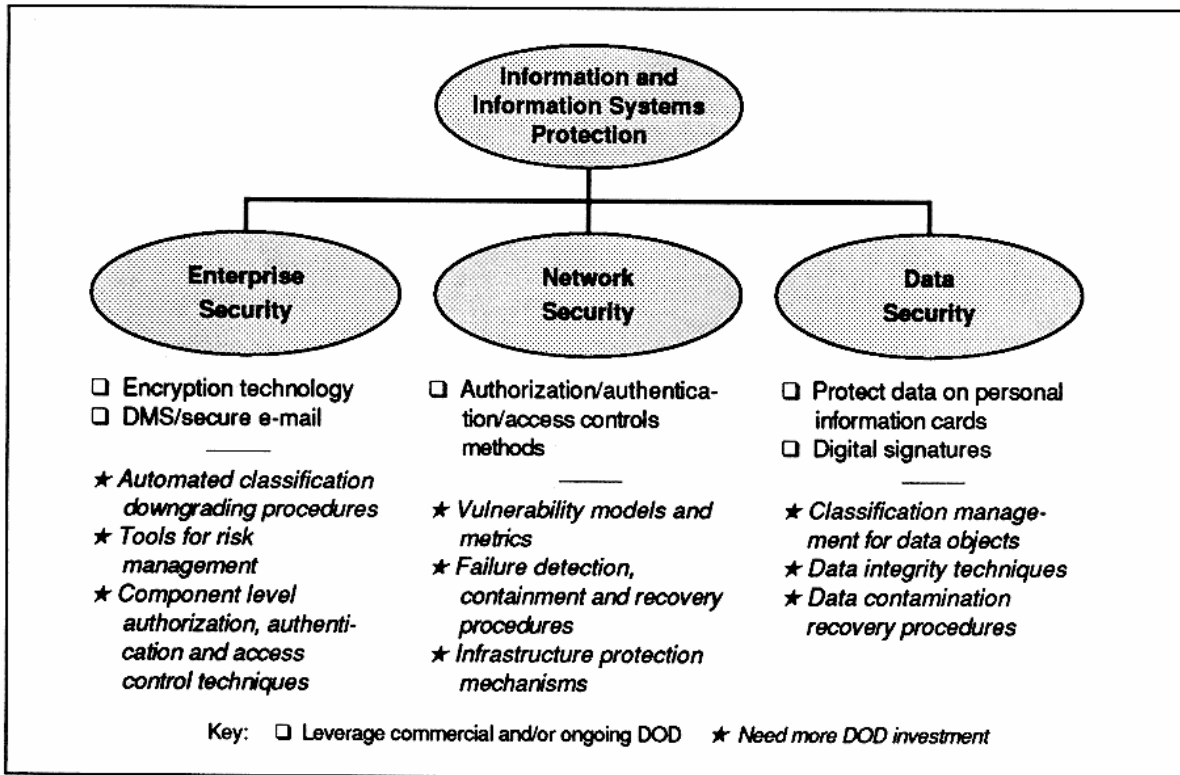
Figure 29

Architecture and Technology – 2

- **Technology is not a major impediment to information dominance on the battlefield.**
- **The commercial information industry leads in technology and research investment.**
- **Information technology is available globally.**
- **DOD should:**
  - Invest in military-unique information technology R&D.
    - Give special attention to information protection technology.
  - Use the best commercial technology.

Action:
DDR&E ensure that R&D strategy capitalizes on commercial technology and focuses DOD investment in military-unique information technology.

Figure 30

Prioritize R&D Investment with Focus on Military-Unique Information Technology

Finally, I started the presentation today with this chart (figure 2). Just to remind you that this is where we're coming from, our recommendations were to try to make that joint warfighter a more informed customer so, in fact, he can help us build this plug-and-play world of modern C⁴ISR capability, and be able to plug and play instead of being dependent on the Cold War systems we built. I didn't brief you much

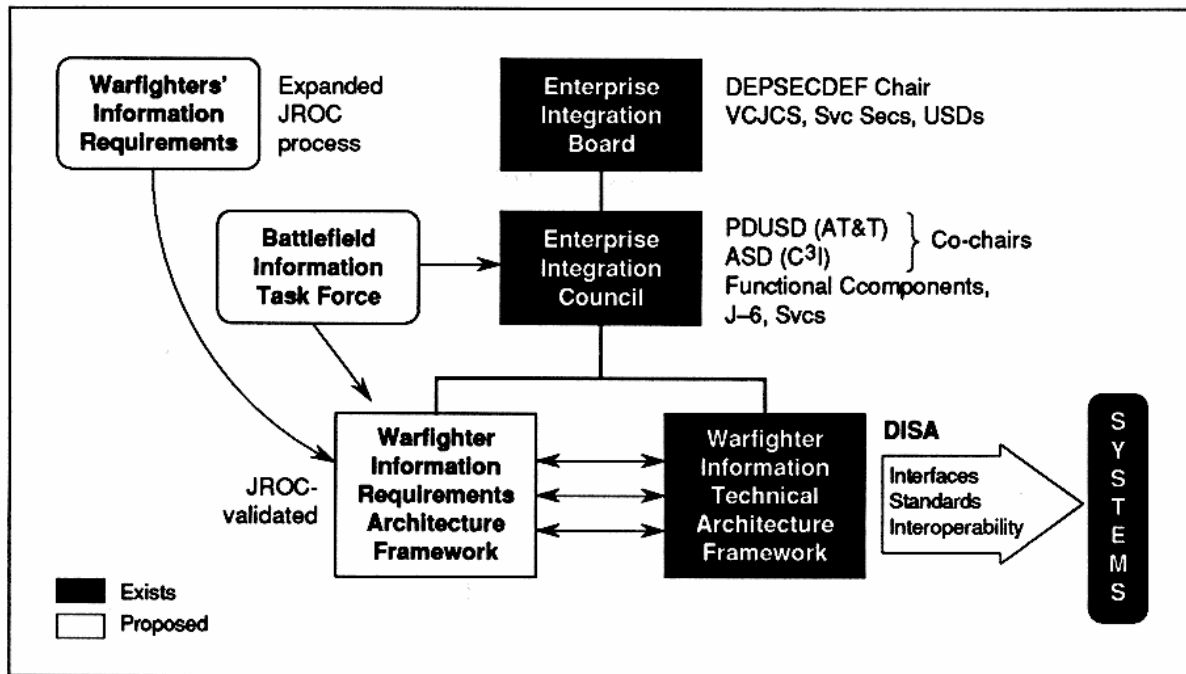**Figure 31**

Structure Concept for Improving Our Warfighter Information Infrastructure Management
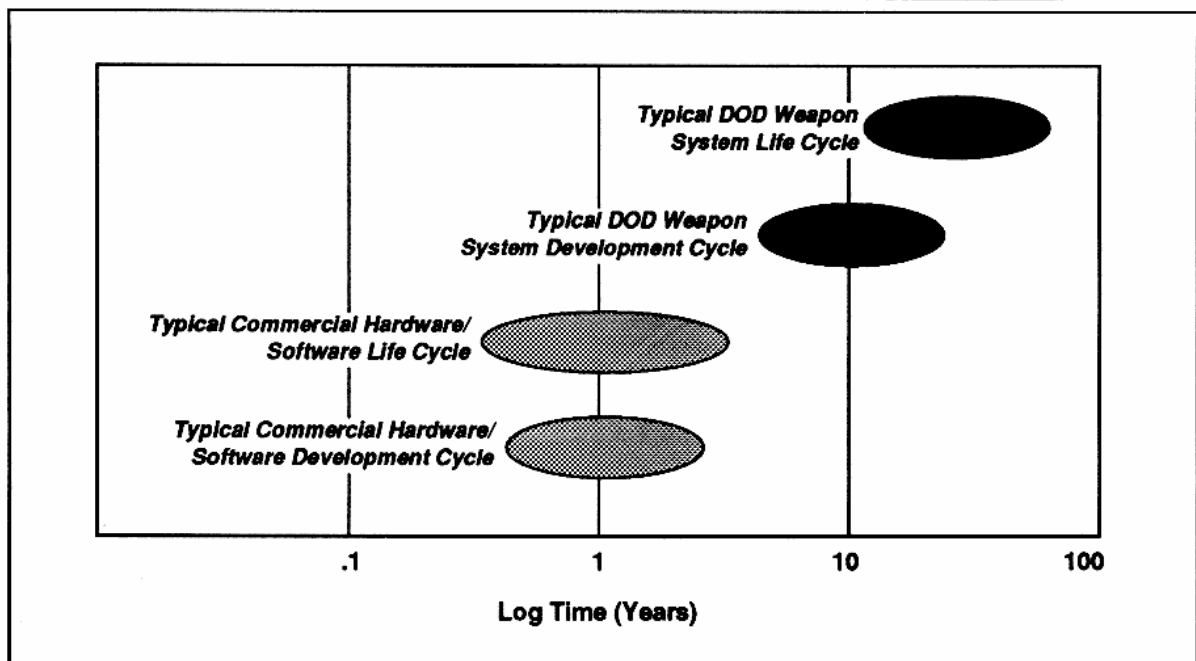

Figure 32

**Rapid Commercial Information Technology Evolution Must be
Infused Into DOD Systems**

Figure 33

Reform Warfighter Information Infrastructure Management

on the last two portions of the study because we ran out of time, but I think you have the heart of the issues in the first two.

That leaves us about 10 minutes to wrap up.

Student: Sir, you talked about information broadcasting using direct broadcast satellites and I just wondered if that's meeting our security requirements.

Rosenberg: It's all enciphered information when it needs to be. Not information in the open.

Student: My question, though, is, are we that confident about our enciphering capabilities that you put the whole endgame, everything you know, up in the air?

Rosenberg: No. We're not confident that no one can decipher it, but we're confident that we can put it together in such a way that we will be able to maintain dominance over them. A concept that I really didn't talk much to because I was getting behind is vulnerability management. There was a bullet on one of the charts (figure 20). Let me just describe the concept a little bit further.

In the Cold War we operated at what we call a "system-high" security level in order to protect ourselves from the Warsaw

Pact and the Soviet Union—the bad guys—and protect sources and methods and all that. Since multilevel security systems were really an unattainable thing at the time, we used to classify everything at the highest level. That made it absolutely impossible for a warrior to get a job done without a lot of problems.

The concept we talked about here, which, in fact, is being employed today, is to put the vulnerability management decision in the hands of the warrior. That is to say, if he's a land combat commander, and he gets on the drive and he is inside the enemy's information cycle and the operational tempo is such that he knows that he's going to reach his objective very rapidly, it's up to him to decide what blue force information bits are at risk as well as red force information bits. When he sees he's nearing a stalemate, or he sees he's in trouble, he should tighten that rheostat up, and cut that information flow down.

Student: Cutting it down, he has some control over it.

Rosenberg: One of the things that the task force is very sensitive to is this whole issue of defensive information warfare by the bad guys, and we're just as vulnerable to it as they are unless we provide protection. We want the commander to have

292

flexibility. We don't want somebody at NSA or CIA or DIA predetermining what he can and can't use. When I went to the Bosnia theater, aboard the *Teddy Roosevelt* there was secret imagery coming aboard ship through SCI pipes, special compartmented information pipes, into a vault that was at a classification level that our F-14 and F-18 pilots and crews were not allowed to look at. Even though they had Secret clearances, they couldn't have access to that vault.

I don't know how many of you saw the movie "First Knight" (I'm using Hollywood vignettes here). "First Knight" is a new movie about Sir Lancelot and Lady Guinevere. I don't know how many of you are history students and know much about medieval gauntlets, but they killed 9,000 out of 9,001 people who tried to get through them. Sir Lancelot runs this medieval gauntlet to survive and get a kiss from Lady Guinevere, and I told Secretary Perry, "Going from national intelligence to the hands of a warrior who is trying to carry out the orders of his President is like running a medieval gauntlet."

What we have done in the Bosnia theater is do away with system-high classification. All information going to our warriors and our coalition partners is going at the Secret, releasable NATO, level electronically, from point of origin to those warriors.

Oettinger: Rosie, over the 16 years that we've had this seminar, I'll bet you there hasn't been a year when somebody hasn't said that the green door problem was solved ...

Rosenberg: I didn't say it was solved. It is breached.

Oettinger: How come it keeps ... ?

Rosenberg: Would you believe that we are electronically transmitting to the NATO database from the U.S. intelligence databases digital imagery and a lot of NSA SIGINT information, except for some of the most sensitive COMINT? I'm just telling you it's being done.

Our big concern is the Russians have those same terminals, and so, that's part of the challenge of implementation. These were some of the recommendations that were made out of this Bosnia task force I was on. Our key recommendations were to tear down the security barriers and allow our coalition partners and our own warriors to have the information they need in a timely manner to do their job.

This takes me back to the Bosnian Serbs. They were inside our information cycle time. They had information dominance. The only way to get it back was to get rid of sneaker nets and fat fingers. I apologize to those of you who don't come from DOD. Sneaker nets and fat fingers are what, in the civilian world, you would call islands of computers connected by miles of tennis shoes. That's the way many of our command and control systems work in DOD—as islands of computers connected by miles of tennis shoes and kids fat-fingering in data by hand—46 target coordinates times 12, that's 480 digits—at a 20 percent error rate. Pretty soon the enemy's inside your information cycle time. So we said, "Do away with those barriers. Get the information all electronically connected. Break down the security walls so that it can happen, because we don't have these fancy multilevel security systems."

The other thing we said to do is to break down the two separate worlds. Since there are some intelligence guys in here, one of the problems we have is that everywhere you go in the DOD world, you get this thing called the "J-2 ops intel cycle." Then you have another thing called the "J-3 ops cycle," and you get briefing after briefing from DIA, CIA, NRO, CIO, and everybody else in the intelligence business saying, "We are the glue that binds it together." Wrong! What I've been talking to you about for the last two hours is an integrated J-2/J-3/J-6 operations cycle. That's where the Department of Defense is headed. It's a long road to go. There are still a lot of people fighting it. We are trying to find positive incentives to make people want to play together.

Student: We had a speaker a few weeks ago, Admiral Cebrowski, who talked about the concept of autonomous operations, and how higher authority resists giving people at lower levels the information they need to operate on their own.

Rosenberg: Yes, hierarchical. A lot of folks don't want the lieutenant to have the information. They want to control all that. Now, those are called rules of engagement. After I leave, the guys who wear uniforms when they're not in this course can let you know whether I'm crazy or not. But what leadership is all about in industry, in the military, and everywhere else, is persuading people positively to follow good rules, and what this new concept talks about is the kid down at the lower level not stupidly doing something with information he now has at hand, just because the information is there. He still has order and discipline to follow through on the set of rules that come from above. They're called rules of engagement. Up that chain of command, what this new concept requires is more empowerment by the leadership to allow the people below them to take advantage of the information they now have in their hands. It's a concept that will enable us to have information dominance of the battlespace, whether it be peacekeeping, peacemaking, disaster relief, getting hostages out of Entebbe again, or whatever. It's like that colonel who said, "General, those are crazy ideas." I can't talk to him; he's senile just like I am. I'm talking to the younger generation.

Oettinger: On that note, sir, we thank you very, very much for a fantastic discussion. I have for you a very small token of our appreciation.

INCSEMINARS1996