

INCIDENTAL PAPER

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

**FFRDC Business at MITRE
Victor A. DeMarines**

Guest Presentations, Fall 1997

Jr. Robert R. Rankine; Victor A. DeMarines; Keith R. Hall;
William R. Clontz; Kenneth A. Minihan; Henry A. Lichstein; John
J. Sheehan

January 1999

Program on Information Resources Policy



Center for Information Policy Research



Harvard University

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

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

Copyright © 1999 by the President and Fellows of Harvard College. Not to be
reproduced in any form without written consent from the Program on
Information Resources Policy, Harvard University, Maxwell Dworkin 125,
33 Oxford Street, Cambridge MA 02138. (617) 495-4114

E-mail: pirp@deas.harvard.edu URL: <http://www.pirp.harvard.edu>
ISBN 1-879716-54-2 **I-99-2**

FFRDC Business at MITRE

Victor A. DeMarines

Victor A. DeMarines is President and Chief Executive Officer of The MITRE Corporation and a member of the MITRE Board of Trustees. He also directs the Department of Defense Command, Control, Communications and Intelligence Federally Funded Research and Development Center, MITRE's largest business unit. He has worked in the C² field in various capacities with increasing responsibility throughout his MITRE career. He managed MITRE's Bangkok site from 1967–1969, served as technical director for Intelligence and Electronic Warfare Systems from 1985–1988, was vice president of the C³I Group for Air Force Systems from 1988–1990, senior vice president and general manager of MITRE's Center for Integrated Intelligence Systems from 1990–1994, and executive vice president from 1994–1996, when he was promoted to president. His technical activities include a particular focus on networks and distributed computing, and he holds patents on local area network techniques. Mr. DeMarines has served on many study groups within the national security arena, and belongs to various industrial associations involved with national security and data processing. He received a B.S. in aeronautical engineering from Pennsylvania State University, and an M.S. in electrical engineering from Northeastern University.

Oettinger: We will dispense with a long introduction, since you have seen Vic's biography. I wish to express my great personal pleasure at having him here today, since by one of those marvelous acts of fate our professional lives have been intertwined on and off for many, many years, and it's a pleasure to have you here today.

DeMarines: The background here is going to be a little challenging to present. The people from the U.S. military contingent are probably very familiar with The MITRE Corporation, but for those of you who haven't had that pleasure, I'd like first to explain where we fit into the scheme of things and why we're unique. It's difficult to talk about the subject of command, control, communications, and intelligence without an understanding of how the government goes about acquiring such capabilities and The MITRE Corporation's role in this endeavor.

First, I'd like to provide a little primer on FFRDCs, or Federally Funded Research and Development Centers (figure 1). I will go through what MITRE is as quickly as I can, but I think the most instructive thing we can do is talk about some examples of how MITRE interacts with DOD programs in

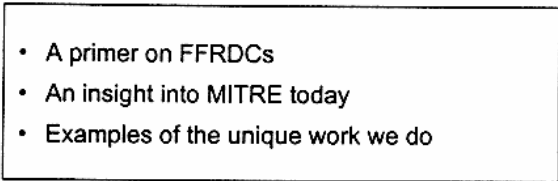
- 
- A primer on FFRDCs
 - An insight into MITRE today
 - Examples of the unique work we do

Figure 1

A Presentation in Three Parts...

command, control, communications, and intelligence. I hope this stimulates some discussion. I've been a part of this seminar off and on, and I've found that you don't have to encourage a lot of discussion. It sort of comes up, and I sure hope that continues today.

Oettinger: These folks are not shy.

DeMarines: That's good.

So, what is an FFRDC? It is a Federally Funded Research and Development Center (figure 2). In the United States, the first one of these was created around World War II. Lincoln Laboratory is the oldest survivor. Lincoln is managed by the Massachusetts

What is an FFRDC?

- It's a Federally Funded Research and Development Center
 - First ones created during World War II; Lincoln Lab is the oldest survivor
- Created to provide a technical capability that private industry and government labs did not have
 - Example: Lincoln Labs brought scientists to work on the war effort
- These reasons exist today, but roles have expanded

Figure 2
An FFRDC Primer – 1

Institute of Technology; therefore, it's MIT Lincoln Laboratory. MITRE was created from Lincoln to provide the government a capability it would not otherwise have. I'll go on to explain what that means. But these reasons have expanded over the years since the war, and I think you'll find it kind of interesting.

There are more than 40 FFRDCs in the country today (figure 3). You know you are one when you show up on the National Science Foundation list. There are 12 in the Defense Department. The Department of Energy has a large number—Sandia, Los Alamos, Livermore, and Oak Ridge—that are involved in the nuclear energy problem. Historically, that's how thermonuclear bombs have been built in this country. There are health-related FFRDCs. Also, NASA sponsors the Jet Propulsion Laboratory that has had a lot of successes in space flight. The FAA sponsors one that is part of The MITRE Corporation, which is called CAASD (Center for Advanced Aviation System Development), and I'll touch more on that later.

We're here to talk about the Defense Department FFRDCs primarily, and again, we break these down. There are 12 of them, and the DOD pays around \$1.2 billion a year for 6,000 technical staff divided among these 12 organizations. You've heard of some of these. RAND runs three FFRDCs: one to support the Army at Arroyo Center; Project Air Force, and the National Defense Research

Who's an FFRDC?

- There are about 40 FFRDCs
 - Listed in NSF
- Four groups of FFRDCs:
 - DOD sponsors 12 FFRDCs
 - DOE's "National Labs" are FFRDCs (Los Alamos, Sandia, Livermore, Oak Ridge, etc.)
 - A number of small, health-related FFRDCs
 - NASA sponsors JPL; the FAA sponsors CAASD; and OSTP sponsors CTI
- DOD's FFRDCs (\$1.2B per year; 6,000 tech staff)
 - Studies and Analysis: RAND (3), IDA, CNA and LMI
 - R&D: Lincoln, IDA and SEI
 - Systems Engineering and Integration: MITRE C³I, Aerospace and IDA

Figure 3
An FFRDC Primer – 2

Institute. Then there are the Institute of Defense Analyses (IDA), the Logistics Management Institute (LMI); and the Center for Naval Analysis (CNA). Some are called R&D centers: Lincoln, IDA, and the Software and Engineering Institute (SEI) in Pittsburgh, Pennsylvania. Then there is a category called Systems Engineering and Integration, which includes MITRE's C³I FFRDC, the Aerospace Corporation on the West Coast, and another part of IDA.

The largest of these DOD FFRDCs is The MITRE Corporation. Our defense business is around \$370 million. The second largest is Aerospace, and Lincoln Lab is the third. ...

There are three basic attributes for FFRDCs (figure 4). One is that the core competencies have to be identified. In MITRE's case, it is information technology. Secondly, you have to have what we call "profound domain knowledge." We have to understand the mission from the customer's perspective, and dedicate our work to that mission. Thirdly, a strategic relationship needs to be in place.

We are a technical organization, with an understanding of what it is to run DOD operations. For example, if we're working on

- Three FFRDC pillars**
- (1) Core competencies
 - Core skills: in MITRE's case, information technology and systems engineering
 - Profound domain knowledge: understands mission from customer's perspective
 - (2) Mission: in MITRE's case,
 - C4ISR for the Department of Defense
 - Air traffic management for the FAA
 - (3) Role: Strategic partner with the government
 - No routine services
 - Accountable for mission, not job
 - Continuity of effort
 - Integrates across individual tasks

Figure 4
An FFRDC Primer – 3

an intelligence program, we will have people who understand intimately what the process of intelligence is about. When we're working on a Navy undersea problem, we understand how undersea operation really impacts the overall mission. So, we provide to the government a combination of our operational knowledge and our technical knowledge.

The mission is also specified. In MITRE's case, as I said, we have two of them: one for the Department of Defense called C4ISR—that stands for command, control, communications, computers, intelligence, surveillance, and reconnaissance—and one for air traffic control.

Our role involves a truly strategic relationship with the government. We provide no routine service. We had a lot of discussion over lunch about what you do when you have work that tends to be more routine. The MITRE Corporation and other FFRDCs conscientiously avoid routine service. The idea is that if you can buy it through a competitive award to industry, don't hire the FFRDCs. If, however, you require the unique knowledge that the FFRDCs have, that's when and why you would use them.

We're accountable for the mission, not the job. That would mean that within the strategic relationship, the people who hire us should also appreciate our candor. So, if we

say, "We don't like what you're doing," they need to understand that we're coming from a perspective of the mission, not the job. In some cases, we have been considered disloyal because we would look at a job and say, "Your design is wrong." But that is the way we work in The MITRE Corporation—with complete dedication to objectivity.

Oettinger: Before you move on, if I might just comment on mission and C4ISR. This question of exactly how many letters are in that name is one that should not detain us today, but it is of some significance both technically and especially in the politics of organization. I interrupt mainly to commend to you a previous session run by Dr. Ruth Davis,¹ where the whole session was spent on analyzing whence all our terminology comes and what lies behind it. So, if you're interested in that—as you should be—read Ruth Davis's contribution to one of the earlier seminars.

DeMarines: Now, as you would expect, there is a great deal of controversy surrounding organizations that are not commercial and not government, but somewhere in between, that are commissioned by the government and get their work through sole-source awards.

I've put some bullets down to discuss this relationship (figure 5). There are service industries in this country that constantly ask the government, "Why would you give this work repeatedly to the companies that you have designated FFRDCs, when you can go out and hire us?" This is a continual debate. A good question to ask the service industry is, "Would you really be willing to accept only those contracts that are awarded 'sole source,' engage in no relationship with any other commercial industry, be at the beck and call of the Congress to discuss how big your budget should be yearly, and restrict yourself to contracts with very little fee? If so, why don't you join us and be an FFRDC? You can't have it both ways."

¹ Ruth M. Davis, "Putting C³I Development in a Strategic and Operational Context," in seminar proceedings, 1988.

Views on FFRDCs

- Service industries (PSC)
- Contractors
- Congress
- Project sponsors
- Our people
- DOD
 - 2 DSB task force studies

DSB = Defense Science Board
PSC = Professional Services Council

Figure 5
An FFRDC Primer – 4

What about the big contractors who make things? How do they feel about FFRDCs? In fact, they're very supportive of us, because we provide a technical capability to the government that makes it a smart buyer. It's always good for the industry to be able to sell something to somebody who understands their product, and to discern the differences between a good product and a bad product. So, a TRW executive might be expected to say: "We're very glad to have MITRE involved because in any source selection—picking solution A or solution B—I know that there will be a technical judgment made by people who understand the differences."

How do I know that's true? Most recently, Aerospace Corporation decided that perhaps they would join with SAIC (Science Applications International Corporation) and give up their FFRDC status. This issue was discussed at great length in the Pentagon, but in the end, the very big contractors weighed in and said, "You cannot do that, because we really would like the government to maintain the technical capability within itself to be able to provide this marketplace for American industry." That was enough to torpedo the whole thing, and Aerospace to this day remains an FFRDC for space systems.

Congress sets an annual ceiling on the work done by the DOD FFRDCs. So, Congress can say how big the FFRDC budget ought to be. It's part of an appropriations bill that comes out every year. Congress has sort of a love/hate relationship with us. They love the kind of work we do, but there are lobby

groups who favor more money being given to the for-profit sector. So, we have this kind of issue to work annually.

We were talking over lunch about how our project sponsors feel about MITRE. Since we are limited in how big we should be, the question of how you portion out MITRE becomes a real issue. We are over-subscribed by at least 30 to 40 percent, which is to say that we could make the company very much larger overnight if we were permitted to accede to the demand for us in the marketplace. So project sponsors in fact do like us, even though we sometimes speak our mind as any partner would.

How do our people feel about it? I believe this is a particularly strong point for The MITRE Corporation. When you work there, you have an objectivity that you are asked to maintain, you work on nationally important problems, and by your own practice try to work the leading edge of the issue. That's pure gold for people in engineering technology: to say, "I can work with peers, I can work on interesting problems, I understand the value to the United States or whomever we serve, and I can be objective." That is a very enviable situation, and is the reason for our ability to retain high quality people.

The DOD deals with all of this at the top level and repeatedly, almost on a yearly basis, they take up the issue, "Do we or do we not want to continue FFRDCs? If we feel we should continue them, then how shall they operate?"

Two recent Defense Science Board task forces addressed this subject. One, led by Bob Hermann,² reported, "... The task force is convinced that the current FFRDCs provide critical support to the department, and was reluctant to recommend steps that, in its judgment, would place this support at risk." That was in September 1995. The second one was more skeptical. However, former Under Secretary of Defense for Acquisition and Technology Paul Kaminski transmitted it to Congress with a cover letter that cited FFRDCs as providing "high quality, high-value technical and analytical work that could

² Dr. Robert Hermann was ASD C³I in the Bush Administration and is now chairman of the board, Draper Laboratory.

not be provided as effectively by any other means." This is certainly strong support. Do I take this to mean that's the end of that discussion? No, it's just how last year's evaluation ended up. The debate will continue, as it probably should, to make sure that the government gets what it needs out of these kinds of organizations. I welcome that debate.

Is that enough on FFRDCs, or do we need more discussion? It's not a term that is common outside the United States; nor is not-for-profit business, which is another of our unique identifiers. We are a 501(c)(3), not-for-profit corporation.

Oettinger: That refers to the tax code.

DeMarines: Let me show you our mission statement: "As a public interest company, in partnership with the government, MITRE addresses issues of critical national importance combining systems engineering and information technology to develop innovative, actionable solutions that make a difference."

We operate in the public interest (figure 6). We're a not-for-profit independent corporation. I have a board; I'll discuss that shortly. I can hire, I can fire. We can work only for government and other not-for-all know, information systems are at the heart of all great command and control systems. Components include networks, computers, software, and decision support systems. Where is the focus of research going on in that area? It's in places such as Microsoft,

- Chartered in public interest as a not-for-profit, independent corporation
- Works for government and nonprofits
- Does not manufacture or provide routine services
- Objectivity in its work
- Access to proprietary industry and government information
- Flexibility in use by government agencies

Figure 6
MITRE Characteristics

profits. We can't manufacture or do routine services, but we can build prototypes, which we do all the time, to show our technical feasibility.

Another important characteristic is that we get access to proprietary information. As you Silicon Graphics, and other information technology companies. They have a relationship with MITRE engineers such that we can get advance looks at new products. We also have our own research program whose members have substantive dialogue with them. And so, if you wanted to know what is going on in the information systems business, and what the trend lines are, you would find a very good body of knowledge within MITRE. Those companies will trust us because we cannot ever compete with them, given the very nature of our operation.

Oettinger: Some of you may be dissatisfied with your term paper topics. There's food for thought here for anybody who is interested in organizational behavior and structure and so on, and in the balancing acts that you just talked about. In a sense, it's a trade-off between knowledge and power. They're in the knowledge business, and in order to maximize their effectiveness in the knowledge business they've given up some power—not necessarily out of their own desires, but because they're permitted a certain amount of power in exchange for objectivity about something proprietary, limitations on whom they can work for, and what kind of work they can do. So, there's an interesting set of tensions being resolved by this particular balancing act between access to knowledge and exercise of raw power. Even the market plays are political.

DeMarines: The last point in the slide speaks of flexibility, and there are a couple of examples. When the government needs something it can't otherwise get, it will oftentimes ask for us. So that's why you will find MITRE engineers in Somalia when they have a unique problem, or in Bosnia, in the Gulf War, in Vietnam, or anywhere a situation arises where the government needs some flexibility for highly qualified technical people it can press into service.

But, as I said, we are an independent company. Make no mistake about it. We have a board of trustees (figure 7). If MITRE were a commercial company, there would be a board of directors; when you have a not-for-profit company, you have a board of trustees.

- Dr. James R. Schlesinger, Chairman
- Admiral James B. Busey IV, USN (Ret.)
- Victor A. DeMarines, President and CEO
- Dr. Lewis M. Branscomb
- General Paul F. Gorman, USA (Ret.)
- Dr. William Happer, Jr.
- Dr. George H. Heilmeyer
- Richard J. Kerr
- General Robert T. Marsh, USAF (Ret.)
- William B. Mitchell
- Dr. David V. Ragone
- Dr. Sally K. Ride

Figure 7
Board of Trustees

The board is made up of some distinguished people whom you may have encountered in some of your readings. The chairman is Dr. James Schlesinger, who was the secretary of defense, the DCI, the first secretary of energy, and was the head of OMB.

Oettinger: And a Harvard graduate.

DeMarines: We have other people from academia: an MIT fellow, Dave Ragone; Lew Branscomb, a Harvard professor who was once the chief engineer for IBM; and Will Happer, a physics professor at Princeton. And we have Dick Kerr, once the deputy director of CIA. We also have military people: Jim Busey, a Navy admiral who was subsequently the head of the FAA; Paul Gorman, a four-star general from the Army; and a four-star Air Force general, Tom Marsh. Then we have business leaders: Bill Mitchell from Texas Instruments; and George Heilmeyer, the chairman of Bellcore. Most recently, we signed up the first U.S. woman astronaut, Dr. Sally Ride.

All in all, that's a very interesting set of people from a very interesting set of backgrounds. They challenge the company, and their job is to look out for the public interest. Their bottom line is not how much money we're making; it is: "Is the public being served by The MITRE Corporation? Are we doing the job correctly?" With their backgrounds, you have to be pretty good to prove to these folks that you're doing the best you can do.

We are a company that has two FFRDCs: one for the FAA and one for the DOD (figure 8). We run business sectors: Air Force, Intelligence, and Washington C³, which serves other components of the DOD—Army, Navy, DISA, NSA—and the FAA. This is a \$488 million enterprise with 4,200 people. We have roughly 3,000 technical staff members—people with technical degrees—and that number varies from year to year (figure 9). The policy has been promulgated by the DOD that the size of the C³I FFRDC ought to roughly follow the size of the C³I budget, which is around \$50 billion. Should that go down, then The MITRE Corporation will go down. Should it go up, then MITRE will go up.

Where do we come from (figure 10)? When you hire MITRE, you generally hire a person with industrial experience; a few come from government; and there are some people from other not-for-profits.

We have a relatively senior staff. The predominant skills are in the computer business, as you see: systems engineering, software, networking, communications, et cetera. Two-thirds of the staff have advanced degrees; 12 percent are Ph.D.s, mostly in the engineering disciplines. The figure lists their areas of concentration (figure 11).

Another significant characteristic is that we work where the problem is. These are the sites that we run (figure 12). We find an interesting set here. We work for the Army at Fort Huachuca out in the desert. We work for the major commands. Down at MacDill AFB, it's SOCOM and CENTCOM. We work for the Navy in San Diego and Norfolk, and for the Air Force at Dayton, Ohio. We also go to a manufacturing plant like Boeing up in Seattle where they build the AWACS

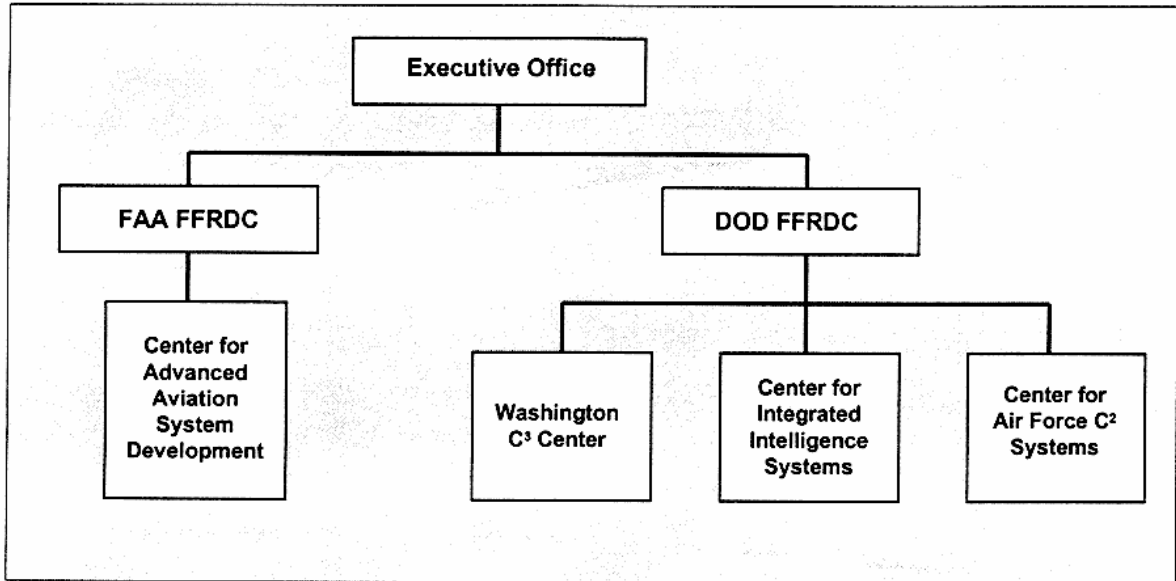


Figure 8
MITRE Partners with DOD and FAA

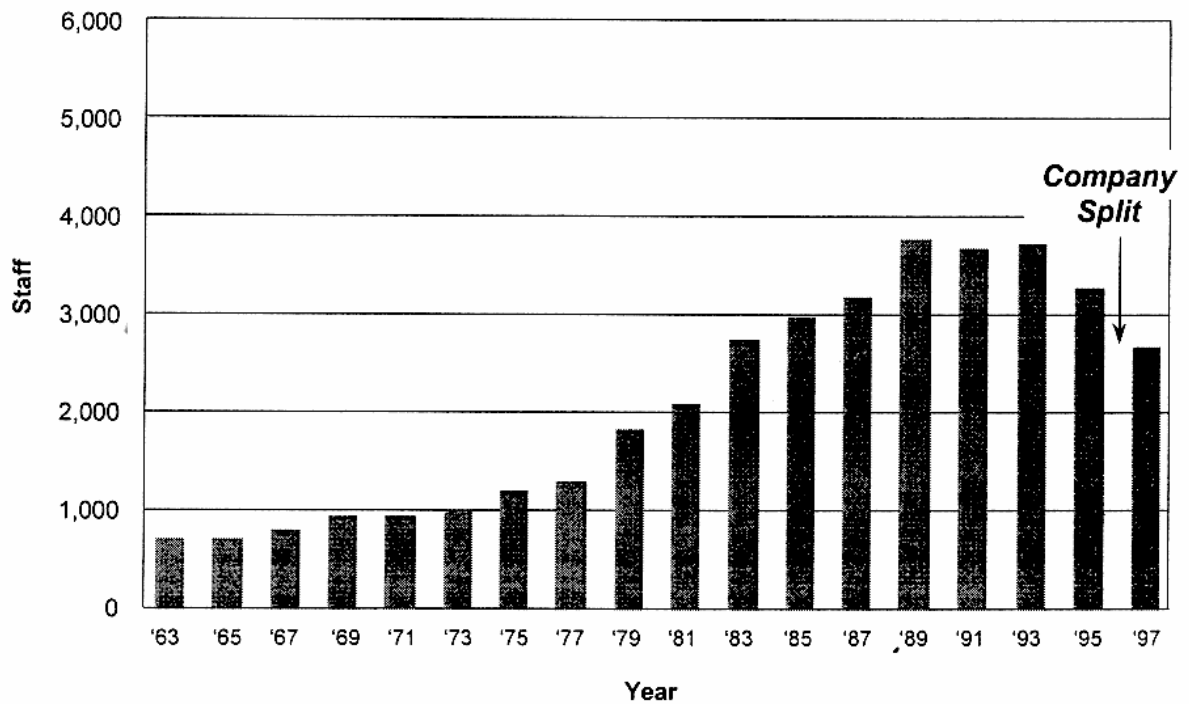


Figure 9
Staffing Levels Adapt to Government Needs

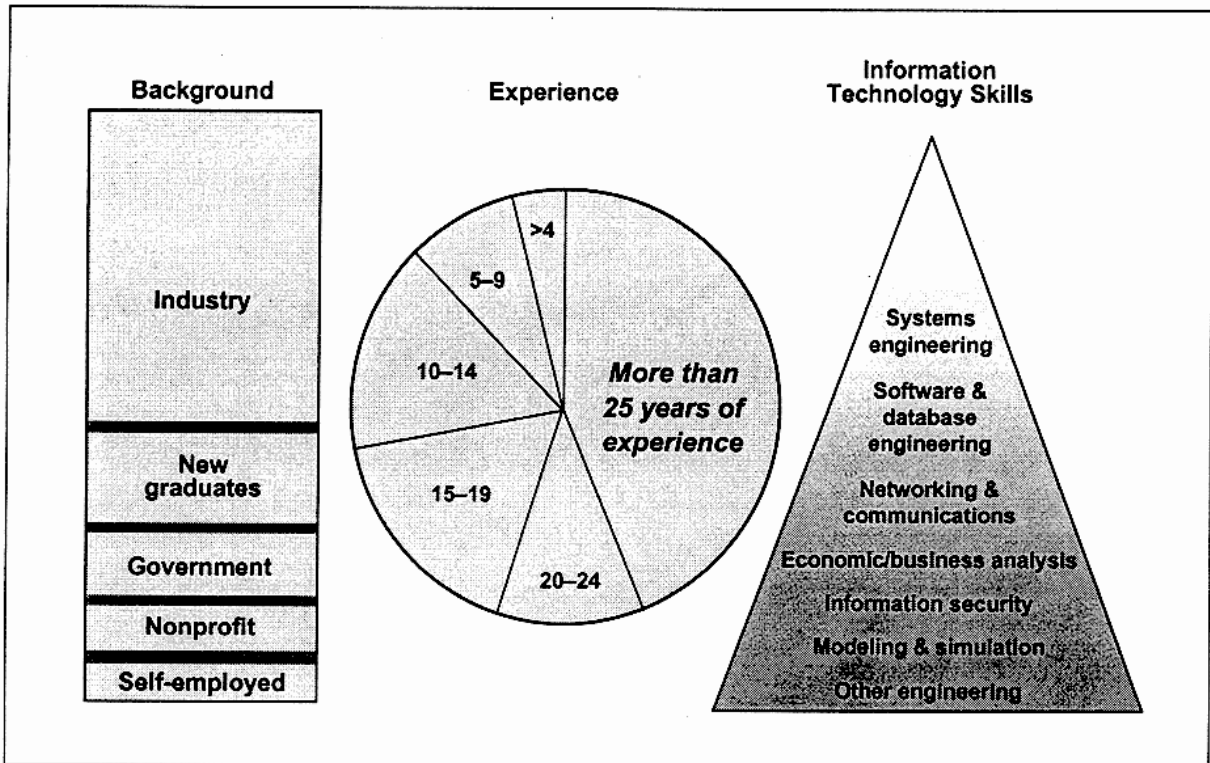


Figure 10
Staff Profile

Area of educational degree

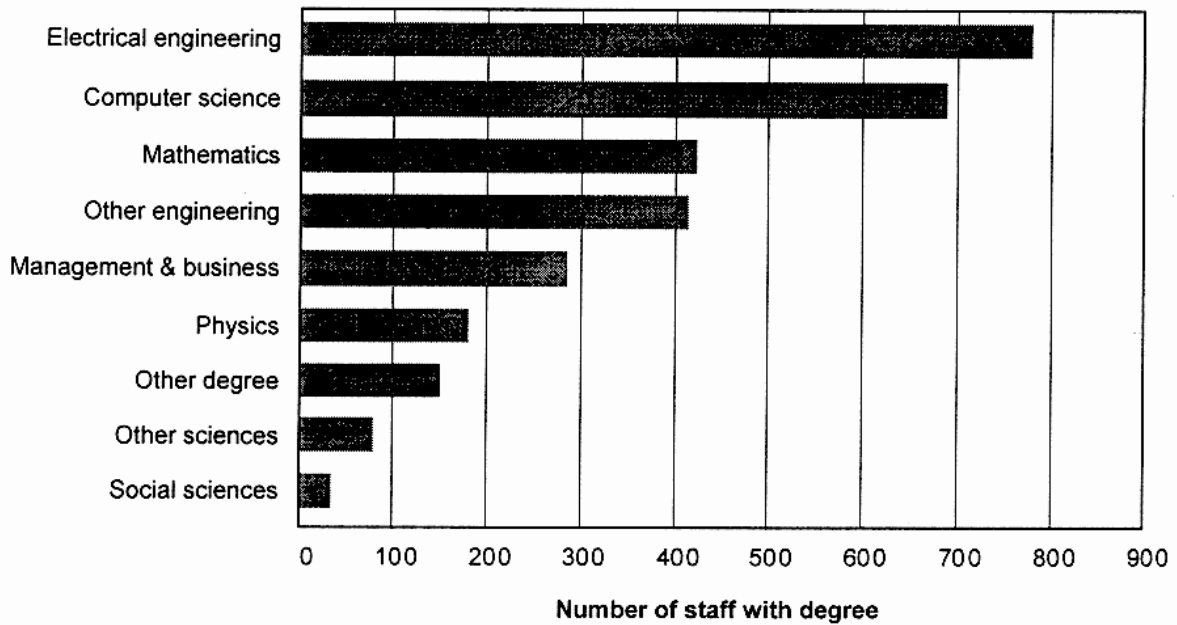


Figure 11
Staff Education

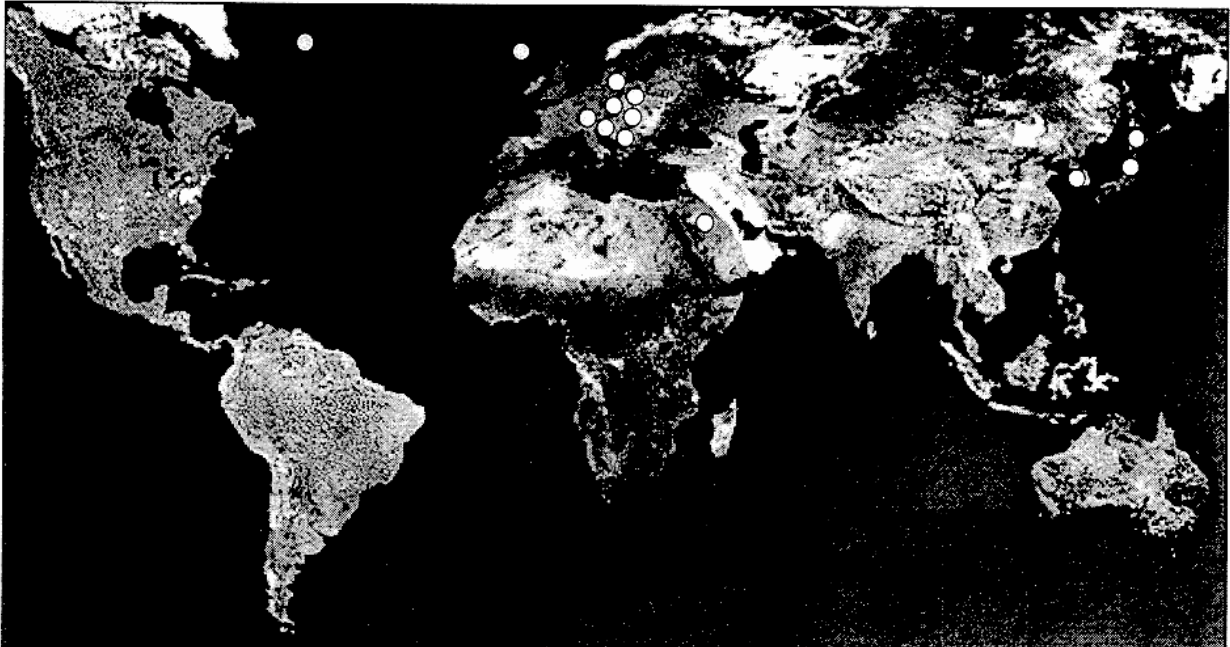


Figure 12
MITRE Locations

(Airborne Warning and Control System) aircraft. Internationally, we have sites from as far north as Greenland and as far south as Saudi Arabia. There are several in Europe, as well as in Korea and Japan. About 60 sites make up The MITRE Corporation—a very distributed company.

Our technology program is vital to our operation (figure 13). Part of being an FFRDC is that we need to maintain our technical quality to be absolutely preeminent. Our government sponsors recognized this need, and have agreed to give us an account of roughly 6 percent of our revenue to be our own discretionary investment in IR&D. We will invest in areas where we think the government needs to be technology-wise in a few years even before it is apparent. And we use this investment to bridge and to complement our commercial technology investment.

You'll notice that we are now very much into computer and information systems, enabling technologies, and sensors. If you took this same chart only about five years ago, you would find that we were more heavily involved in radar systems, but the command and control world has changed so much into

an information world that our investments are now clearly in this area.

These are the DOD sponsors for whom we work (figure 14). It's like a Who's Who of command and control: Army and Navy, Air Force, major commands, Office of the Secretary of Defense (OSD), et cetera.

We also work for the FAA, and for the international community in air traffic control (figure 15). That's another interesting situation. There is strong agreement within the air traffic control community for international commonality in operational procedures. Our FAA encourages MITRE in this regard. We find ourselves in Canada, as they privatize their air traffic control system, or in Mexico, as it tries to build a new set of airports around Mexico City. Egypt is building a whole new air traffic control structure. We hold contracts directly with Belgium, Japan, Taiwan, Singapore, and others in the interest of the worldwide aviation community.

I'm going to talk about our work now. In the interest of time, I'm going to portray only one small example of our FAA work (figure 16). The FAA has a system that has not changed much over the years. Airplanes go

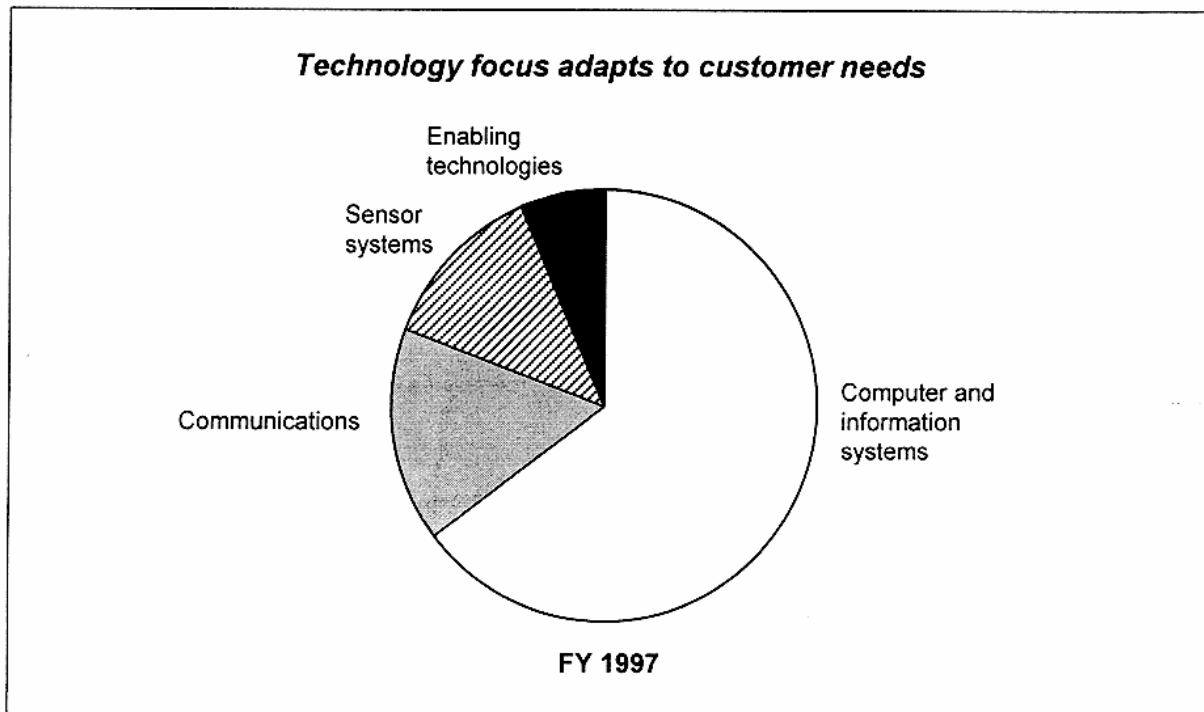


Figure 13
Technology Program

- U.S. Air Force
- U.S. Army
- U.S. Navy
- U.S. Marines
- Defense Information Systems Agency
- Advanced Research Projects Agency
- Defense Intelligence Agency
- Unified commands
- National Security Agency
- Office of the Secretary of Defense
- Ballistic Missile Defense Organization
- U.S. Government (classified)

Figure 14
DOD C³I FFRDC Principal Clients

from point A to point B by following established routes in the sky. We find that the burden on the air traffic control system increases at about 5 percent per year, and more delays occur as this trend continues.

MITRE is helping here. We've done system models of all the air traffic control in the world: we take all the flights (this information is available from the books you look at to figure out your flight schedule) and run a system model on a computer. We find out some very interesting things. We find that we've got to do something soon, or within five or six years the system in this country will start to incur significant problems, in the sense that the delays will become extremely hard to handle. We helped coin the term "free flight," and we started to get the FAA to put some tools out that will help bring about more direct routing. One is called the User

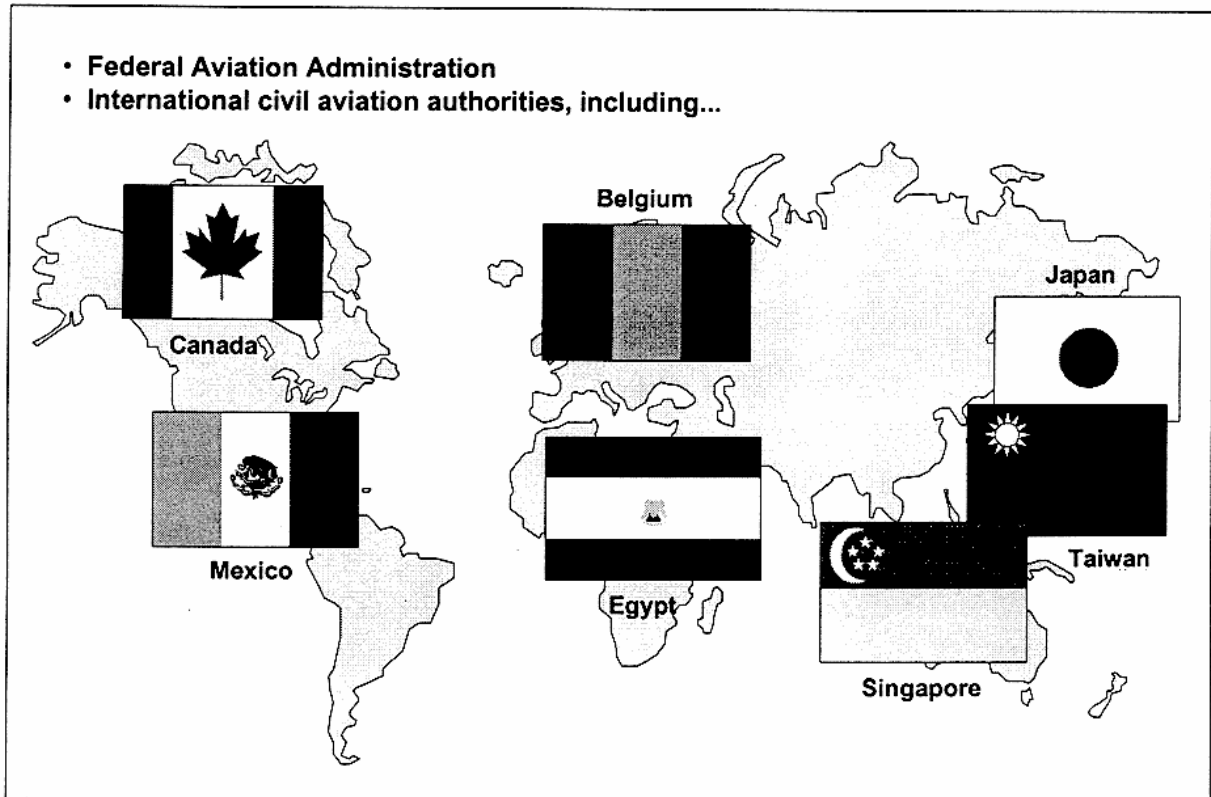


Figure 15
FAA FFRDC Principal Clients

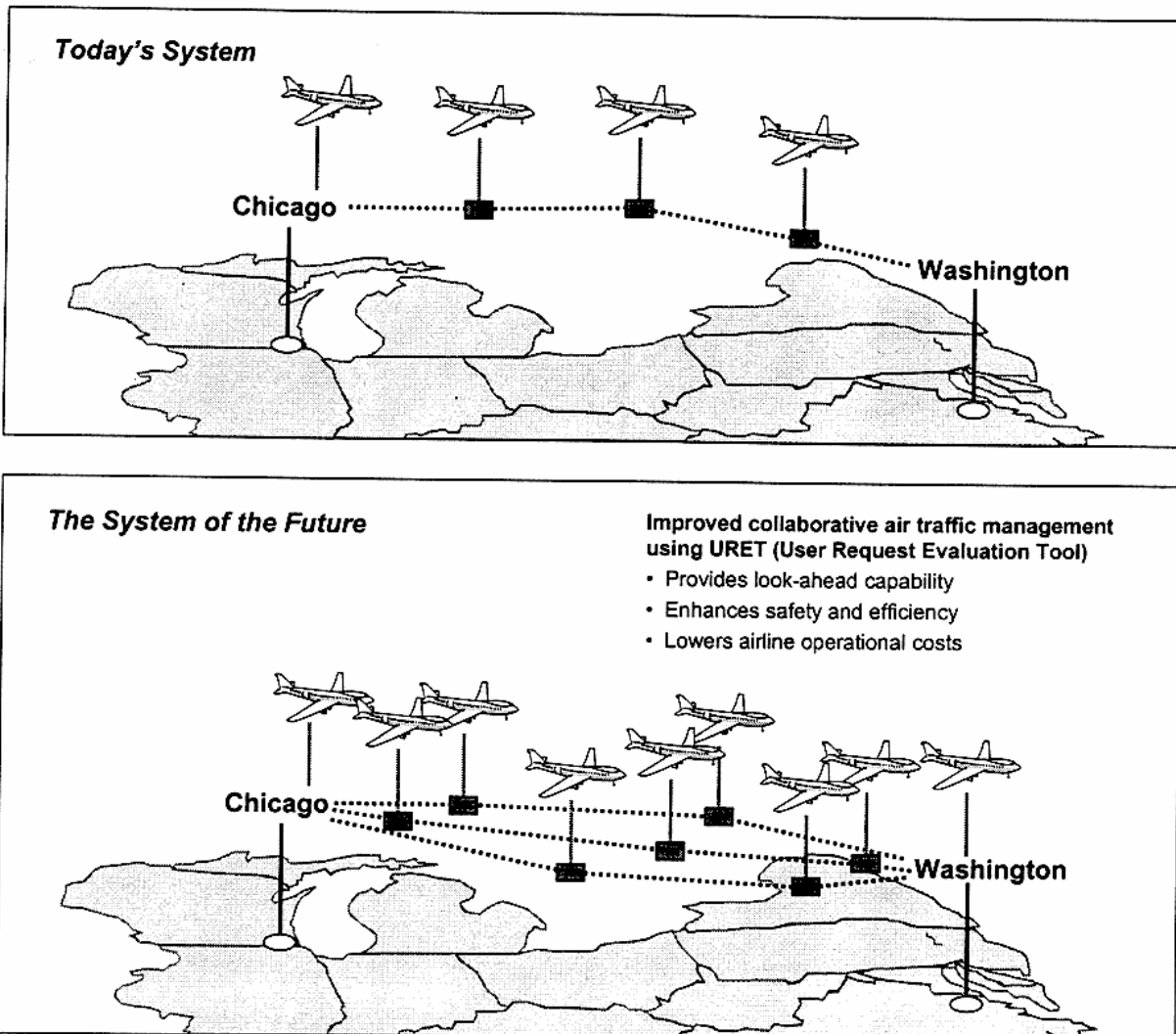


Figure 16

Managing Dramatic Growth in Air Traffic

Request Evaluation Tool; it is now operating in Memphis and Indianapolis, and will be rolled out throughout the country.

This example shows you what the FFRDC can do. It can say to the FAA, "The way you're doing business is really wrong. What you have to do is change dramatically." But, people who have been working with the old system have developed an affection for it, and change always comes hard. We have to use such capabilities as those provided by the Global Positioning Satellite (GPS) system, and high-speed digital communications in order to communicate position, velocity and intent. In time we will be able to eliminate VORs (very high frequency omni range) and

DMEs (distance measuring equipment). You can imagine the reaction that gets out of the established bureaucracy. Collaboration would be a challenge. But that is exactly why an FFRDC is needed. In these kinds of cases, you have to have the courage to be the FFRDC. You have to be able to tell people the truth to make it happen.

Oettinger: Let me probe the limits of that for a second, because you mentioned that at least some of the problems raised have to do with the hub-and-spoke airport arrangements, but that approach wasn't around forever. That's a product of deregulation. So there is a political component to this that says that in

the good old days of regulation and CAB (Civil Aeronautics Board) involvement in routing, you had direct flights. You keep describing this as a technical problem, but since you're agreeing with my historical reading of this, there surely is a political component, and who deals with that?

DeMarines: That's a very hard question. I guess the accepted fact is that it is the way it is. We're not going to go back to more regulation. The whole tendency in government is to get government out of everything it regulates. So, we're going to do hub-and-spoke. Why? Because it's economical for the airlines, and they're going to compete with each other. If you don't do this, then you're not going to be in business.

An interesting aspect about all of this is the word "collaborative." Today, the air traffic control system tends to treat every aluminum tube in the sky exactly like every other aluminum tube. You might have a 747 that is loaded with 300 or 400 people vying for the same slot that you have for a little commuter with two people in it. The airlines scream, "Please don't do that, because you are hurting me economically. Let's make some smart decisions." So, the next air traffic control system will be one of collaboration, where the airline, the air traffic controller, and the pilot form a team to make decisions. We're doing work in that area.

The bridge between government and the airlines and other flyers is a very interesting one. It's a little bit simplistic here in the military. The military own the ground control system when they're fighting in battle. They own the airplanes. They can make system decisions. They'll allocate money for the airplanes, they'll allocate money for the ground systems, and they'll get the system problem solved. In civilian aviation, the FAA—the government—owns the ground system, but it doesn't own the airplanes. So, you have to find some other mechanism to influence the decision, and that's a very real problem.

Oettinger: The collaborative aspects raise another problem in connection with civil aviation. Isn't that like dealing with the National Rifle Association? How do you handle

it politically? I'm sort of interested in this. Is this something that you wrestle with?

DeMarines: We've wrestled with it a lot. For one thing, there are organizations that share a common interest, and with whom we have developed close associations. We have also created a subcommittee of the MITRE board to meet with officers for Northwest, USAir, and American, and people representing the private pilots association, and people representing the manufacturers.

Oettinger: So, your staff is technically oriented, but you're not above having a little on the side—some meeting of minds to set the stage.

DeMarines: That's the point about profound knowledge of how the system operates, complemented by profound technical knowledge. That's the beauty of an FFRDC.

Let's take another example: Task Force XXI (figure 17). A few years ago the Army said that it needed to modernize. You may have heard some Army speakers say, "We need to digitize the Army." What they really mean is that they need to put a system together where they know the location and disposition of all the components. That involves a communications system and GPS receivers on all the vehicles and with the soldiers, and digital links that can tie them all together.

How do you bring all that about? The Army asked us to specify the information architecture for Task Force XXI. We specified the Internet protocol. A principle here is

Enhance Army warfighting capability by digitizing the battlefield

- Specify the tactical Internet to improve warfighter communications
- Create a new acquisition process (10 years compressed to 2 years)
- System engineer the digital battlefield to improve lethality, survivability and op tempo

Figure 17
Task Force XXI

that, with the way the technology goes, you can't afford to do anything that takes a very long time. As you all know, your computer starts becoming obsolete after 18 months, and if you had an acquisition program that was 7 to 10 years long, you'd find yourself buying components that were antiquated generations ago. So, a part of this solution had to be: How do you create something that allows you to evolve? You don't buy a thing or a system; you buy an architecture that allows you to evolve. We helped the Army do that.

Before I leave this topic, contracts were given out to many vendors: TRW, Hughes, and others were involved here. Even though we helped write the specifications for the contractors, and helped look at the designs when they came out, it didn't work when it went in the field. The first time it was tested at Fort Hood, Texas, messages would not go through. These were all signs of protocol and system level issues. So, the government turned to us and said, "We'd like about 60 of your MITRE engineers to pack up their bags and go to Fort Hood, and stay there for six months if necessary until the problem's solved." That's exactly what we did to work out each of these system problems until the Army had a very credible design that worked extremely well at Fort Irwin. You see the Army now briefing Congress about the success of their Task Force XXI effort.

We have another example of how we fit into the scheme of things: AWACS. An AWACS airplane has a radar on top that can look at the airspace and help direct the air battle. There are nearly 30 of them in the world. Today, AWACS is flying in Bosnia and flying drug missions in South America, and now it is being procured by many of our allies: Saudi Arabia, Japan, France, NATO. It is a very successful program, which has been operating for all of two decades. What is MITRE's role in this program?

One might wonder, since we had a successful system two decades ago, why do we need a big MITRE involvement, or to get anybody involved? The answer is: for the same reasons. We need to put in new technology constantly to improve operations and maintenance productivity. This slide (figure 18) shows some of the current upgrades, responsible for about a \$500 million a year procurement.

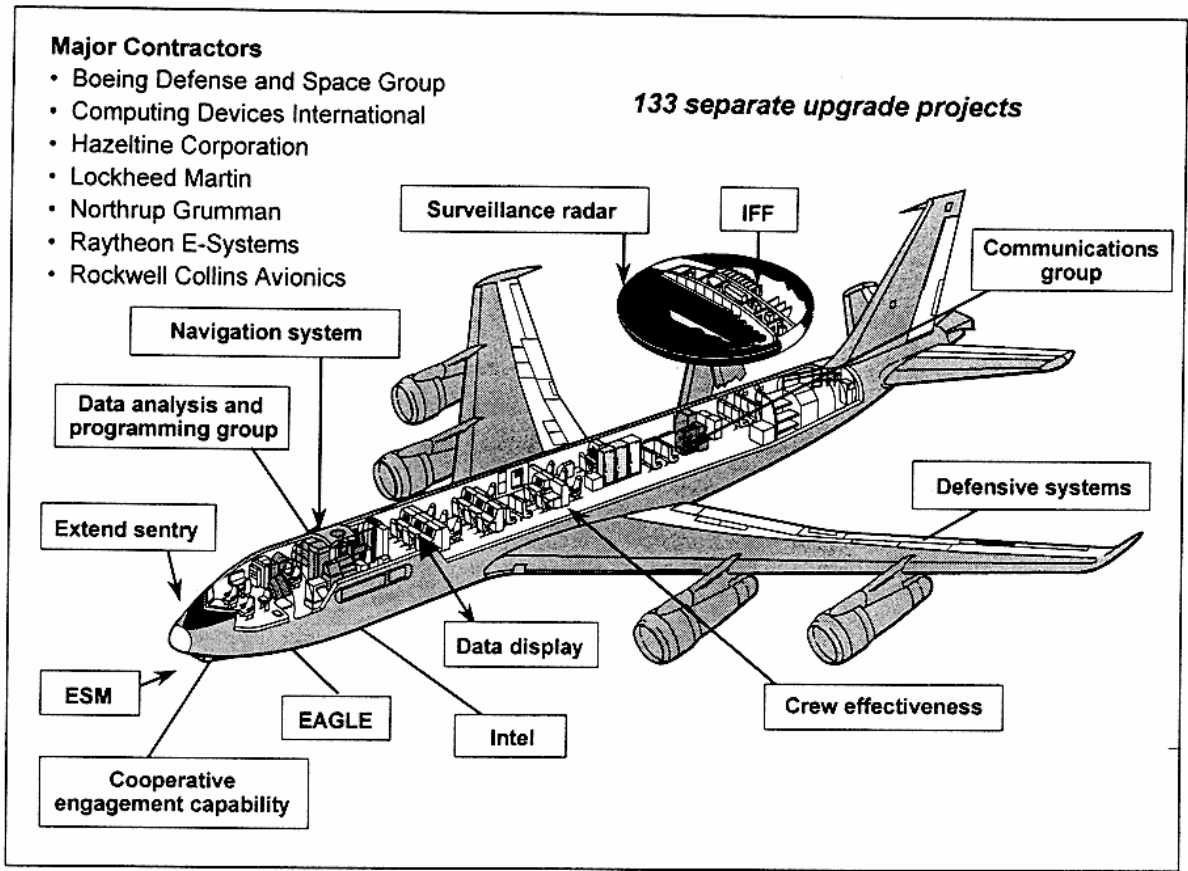
There is a systems program office at Hanscom Air Force Base (figure 19). It has a MITRE program advisor. Each of these AWACS subsystems that I showed on the previous chart has an integrated product team that includes industry, MITRE, and the government. MITRE is on the engineering side of these integrated product teams, and the MITRE program advisor will make sure the designs will interact as they should, and that the timing of things that need to go on the airplane is coordinated.

We don't do this on every program, but MITRE has a very important role at Hanscom. It's not me saying this; you'd get that from the three-star general officer who runs the Air Force Electronic Systems Center. MITRE is ESC's general systems engineer and integrator, and also its systems architect. Our experienced staff at the program offices maintain the programs' history and corporate memory.

I want to make another point. C³I is an extremely sophisticated discipline. Some of the interactive components might look like this (figure 20). Here you see a Rivet Joint intelligence platform, a JSTARS (Joint Surveillance and Target Attack Radar System) synthetic aperture radar platform, a Navy command and control platform, SATCOM, Navy fighters, and other elements. MITRE is involved in all those programs, and we manage a consistent systems engineering approach across them.

This is a subtle point that's not well understood. No one from OSD will pay us to integrate all these systems, but they pay us to work on these systems individually. So, what we must do is manage ourselves so that we can, in effect, operate this way. We try to integrate jointly from the top down, while working from the bottom up on each of our programs.

Here's where we might say: "Well, E-2C, we notice that you're trying to work with AWACS, but you made a decision on a program that we think will not allow the interaction to occur. Maybe it was a decision you made because of dollars or time, but whatever the reason, it doesn't promote interoperability." We would go to the program manager with those issues and the consequences. While industrial organizations seldom present such challenges to program managers, we



ESM = electronic warfare support measures
 IFF = identification friend or foe

Figure 18
U.S. AWACS—Current Modification Programs

have suffered the consequences from time to time and had to leave the job. But we were always brought back.

Oettinger: Can you comment on the “always brought back?” Let’s take for granted that it’s because of the competence, but elaborate a little bit on why the commander of Hanscom Field can’t staff with the military, or hire his own civilians. In other words, say a little bit more about what problem this relationship is solving for those guys that they can’t solve in other ways.

DeMarines: Project leaders—and I imagine that there are many of you in this room—measure success by how quickly they do something, whether they do it within budget and on time (how well, how timely and how

cost effectively). They’re not so interested in solving a large system problem. The commander at Hanscom Air Force Base manages procurements and to every degree possible ensures total system integration. In some cases, however, he doesn’t “own” the total system. The owner may be somebody in the Pentagon, perhaps a program executive officer, and there may be conflicting issues.

Oettinger: So, you’re the only ones who are in a position to get the overview? That would account for why you’re messing around with Joint STARS. But what accounts for your working for Hanscom in the first place, for that piece? Why wouldn’t he have his own civilian or Air Force personnel?

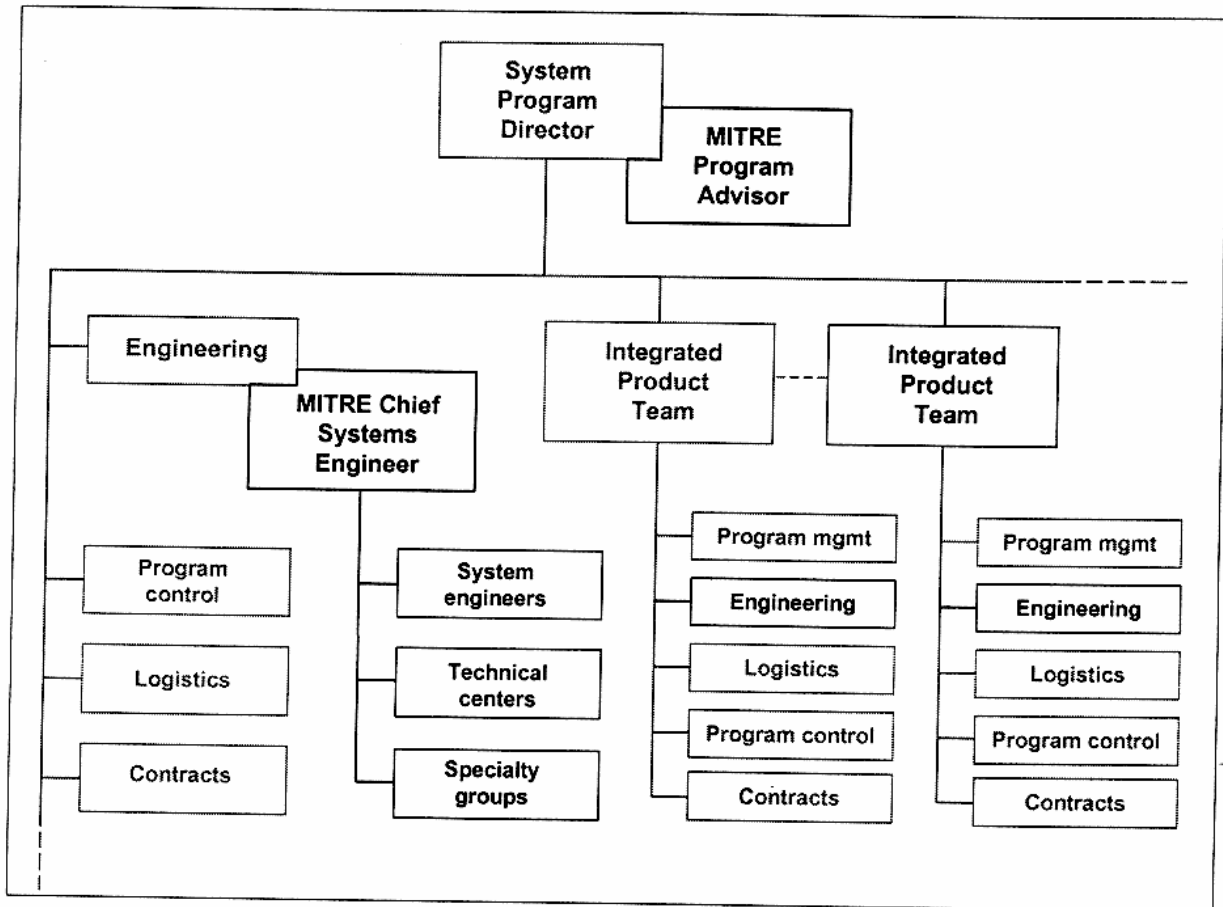


Figure 19
Typical Program Organization

DeMarines: If they had them, or could hire them, that would probably be a very good solution. They made a decision many years ago that they could not hire with the quality and the timeliness they needed, and they'd prefer to use an FFRDC. We could hire and fire. When we started shifting from radar and sensor-based skills to more information technology-based systems, we had a big turnover in MITRE. I went out and hired information systems people and let other people go whose skills, although very credible, didn't match the demand. How would you do that in the government?

Student: Not only that, even if you can hire the government people, when the task they're working on is complete, it's difficult to move them to a new task. You create food chains that last forever.

Oettinger: You're talking about military officers?

Student: The problem with military officers is that they don't stay around long enough.

Oettinger: So the civilians stay too long, and the military officers don't stay long enough. That's what I hear. I just want to make sure that that's clear to some of the folks around this table who don't have the experience with this. The solution to this problem is, presumably, that the people they could hire are the wrong kind of personnel.

DeMarines: You have to match the outside market. As we mentioned, if you pick up the Sunday paper here in Boston and look at the want ads for C++, networking, Internet, et cetera, there are scores of new jobs sitting

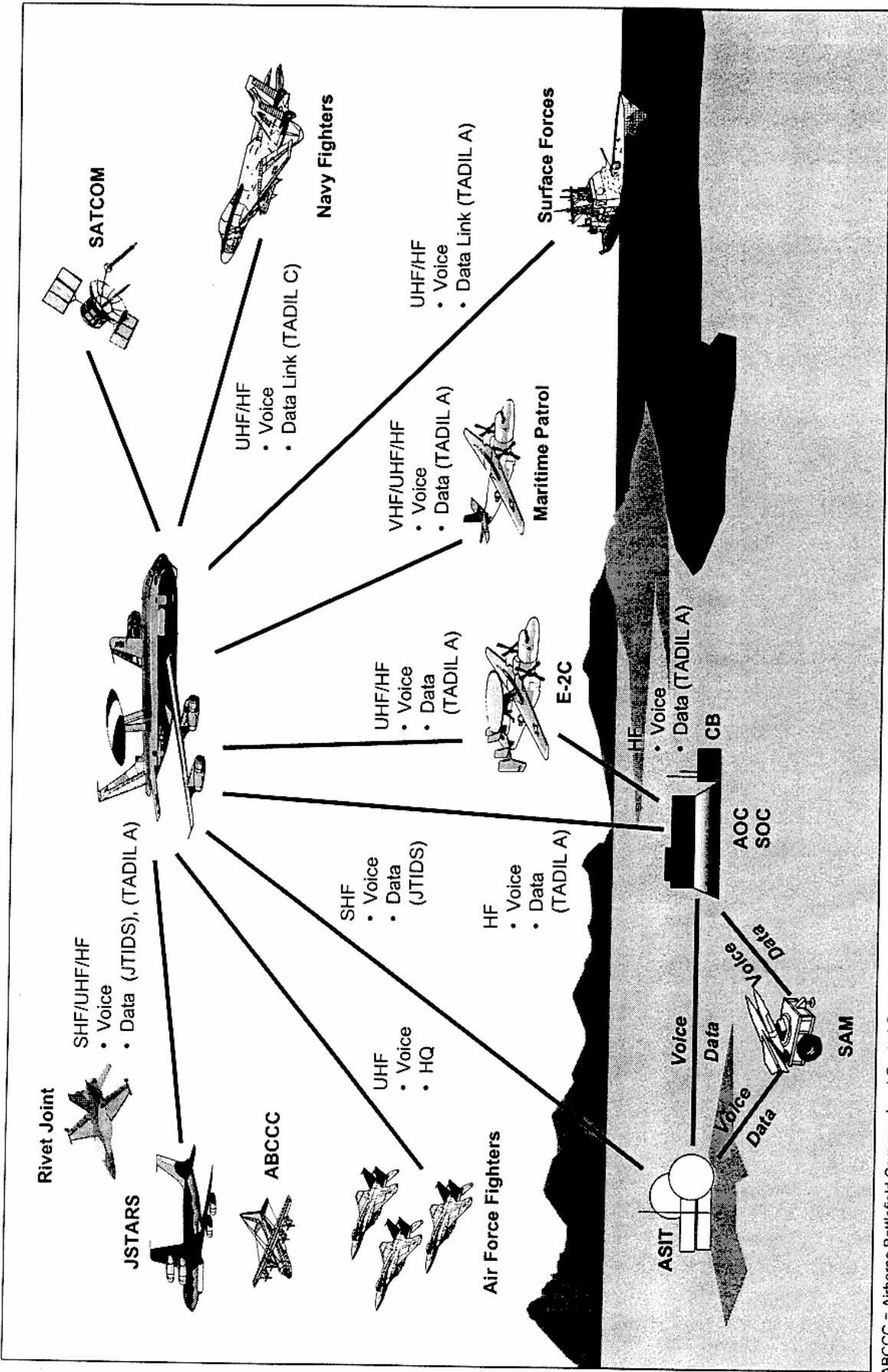


Figure 20
Interoperable Communications: Ground, Air, and Naval Forces

there, with signing bonuses up to \$10,000, and that is the very set of people we need to hire. Can you see the government competing in salary for those? I can't possibly imagine it! But we have to compete for them; otherwise, we couldn't invest in highly qualified technical staff.

Student: Could you say a few words about the E-2C program? What do you do in the E-2C?

DeMarines: The E-2C is the Navy equivalent of the AWACS, which can provide an air situation display. I don't know exactly what we do with the program, but I imagine we do very much what we do with the AWACS on a smaller scale.

We have another project that Tony is particularly knowledgeable about. Some time ago, the deputy secretary of defense asked us to take a look at the Gulf War in a particular way. The press has printed some charges that there were chemical weapons released accidentally during demolition that had some lasting physical effects on people. You may remember the newspapers showing the bunker being blown up in Khamisiyah, which is the place where some people say a cloud developed and that chemicals were released that caused illness. The DOD was having a difficult time figuring out what it knew and when it knew it, and created some controversy because it contradicted itself from time to time. Since we know the intelligence community intimately, we were asked to look into this at all levels of classification open to us, by examining all the traffic and briefing charts, doing interviews, and then reporting to the department what happened when, and who knew what when. That's the sort of study we did. It dealt with command and control aspects, not the physical effects.

There is a political side to it too, because there are some veterans' groups and a White House commission looking at it. There are a lot of stakeholders. The technical side of it is very interesting to me personally. When we looked at all the data available, we found out that there were about 55 million reports that talked about this issue—messages, reports that were actually written, documents like vugraphs, or even handwritten notes. We

knew that we could not escape doing this very completely, so we took the 55 million items and put them on a computer, and then used data mining techniques—some classical artificial intelligence kinds of techniques—to determine relationships among different events, and tried to come up with some conclusions. We are near the end of that, and it has not been without controversy. We don't do analysis for a living; we do it on occasion. But here is where, because we had the intimate knowledge and the technical ability, they asked, "Would you do this?" And of course we took it on knowing that we would get a lot of political heat. There have been some press reports where MITRE was called into question by some people, and praised highly by others. But that's the kind of company we are, and we're going to continue to operate like that.

Student: When is that report on Iraq due out?

DeMarines: That's a very good question, because it's at the very highest level of classification. People are calling for it to be declassified. When that occurs is anybody's guess. Tony, do you care to say anything about this?

Oettinger: Yes, let me comment. I think it's a very important set of topics. I'd like at some point to engage the class in thinking about it and also perhaps at some point to continue the conversation with you. But let me do it in an unclassified vein by taking a very different topic, but with similar characteristics. I refer to the "friendly fire" incident when two U.S. fighter planes shot down the two U.N. helicopters in northern Iraq. The similarity is that both were sort of unfortunate incidents that happened not because of enemy actions. In the Khamisiyah instance, you blew up stuff, and the allegation is that in blowing it up, which was intended to do something to the enemy, you ended up, according to the veterans' groups, making your own people sick.

In the friendly fire case, it's obvious: the intent of the mission there was to keep an eye on the Iraqis; it was not to shoot down friendly helicopters, but it happened. You have in your bibliography Scott Snook's

doctoral thesis³ analyzing this. It was similar: much of the record was available, there was much of the same element that somebody was looking for retribution or a scapegoat or compensation or whatever, so it was a politically loaded subject. The allegations were intelligence failure and/or operational failure, so somebody must be responsible; therefore, whom do we shoot, who will get the money, and so forth and so on. Scott Snook had a particular interest in the friendly fire situation, because as a colonel in the U.S. Army he literally got shot in the ass on Grenada by a U.S. Navy plane. Fortunately he recovered with no more than some residual pain in his gluteus maximus, but since his head was intact, he got very interested in this question of friendly fire. As a matter of fact, just last month or so Princeton University Press contracted to publish his thesis as a book. That book will be part of a larger literature on what one of the grand gurus in that field, Chick Perrow, calls something like "unavoidable accidents" or "natural accidents."

Student: Normal accidents.

Oettinger: Normal accidents, yes. The issue is that when you start poking around one of these things and looking for particular culprits, they are sometimes not findable. Yet, on the other hand, it's not that it's fate. You can't just say kismet, or the will of God, or something. But when you start looking at organizational issues going way back, personal responsibility, not necessarily involving dereliction of duty, et cetera, the first question is what might you do that would reduce the probability of stuff like that happening. One of the conclusions that Snook draws is that scapegoating is exactly the wrong thing, although that is what is most frequently done. Tightening up the rules is the wrong thing, although that is also what most people have done.

I don't know exactly what inferences will come out of this, but the point is that the literature of normal accidents, if you will, is a scattered one. There's Perrow's stuff; there's

this report, if it ever gets declassified; there's Scott Snook's work; there are some people at MIT working on nuclear accidents; there's the woman who's also in your bibliography, Diane Vaughan from the University of Chicago, who did the book on the Challenger disaster.⁴ But they tend to be centered on particular incidents.

I guess the thing that I would want to get you interested in is the notion that you can't prevent accidents totally. That's part of the message. But you might be able to reduce the probability, and if you think of wars or other incidents as accidents that happen, then lessons out of the "normal accident" literature might provide clues as to how to do the intelligence better in order to avoid that kind of accident. Again, that's no 100 percent guarantee, but these accident books have patterns of thinking that I don't find normal in intelligence, command, and control circles. I sense that there may be a whole bunch of ideas that are worth mining. Anyway, I commend that to the class as a part of the bibliography that you ought to take a look at. There is a section, if you'll go back to one of the earlier handouts, on the accident literature. You'll find Snook and Vaughan and Perrow listed. Vic and I could have a conversation about it some other time.

DeMarines: It's not an accident. The Khobar Towers incident is one that had a far-reaching effect on the senior military. It's gotten to the point where the Air Force Chief of Staff resigned because of it. I was down in Tampa talking to General Shelton, who is now Chairman of the Joint Chiefs, when he was running CENTCOM. He said that after Khobar Towers he would get five or six messages a day asking him to take responsibility for things that did not follow the rules. "I know we're supposed to have a 10-foot fence, but all I have is chain link for an 8-foot fence. Can I have your approval to substitute an 8-foot for a 10-foot fence in this particular instance?" He said he put up with that for

³ Scott A. Snook, "Practical Drift: the Friendly Fire Shootdown over Northern Iraq." Ph.D. dissertation, Harvard University, 1996.

⁴ Charles Perrow, *Normal Accidents*. New York: Basic Books, 1984; Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago: University of Chicago Press, 1996.

three months, and he just said, "We all have to take personal responsibility." The idea of responsibility and military judgment is very interesting. If you make it such that it is all rule-based, it will become a challenge to the military, which needs to be creative and aggressive.

Onward! I don't know if there are any intel people in the room, or if you've heard of Intelink, but here is another interesting situation (figure 21). The Defense Intelligence Agency (DIA) has delegated responsibility out to different commands to develop intelligence in their particular areas of interest. So, if you're in Korea, you might be looking at intelligence on North Korean airplanes and ships. If you're in Europe, you might be looking at something else. DIA would take the data back, produce the intelligence reports, and distribute them out to the field. But, that whole structure of intelligence distribution can be very slow. We engaged this problem, knowing the intelligence community, and knowing the capabilities and potential of the Internet.

We bridged those two. Keith Hall, who will come in to talk with you, is very much a part of this, as is a fellow named Steve Schanzer.⁵ He said, "This is all wrong. If we could make people who develop intelligence, wherever they may be, stand up for their product by going on record and putting it on the Internet server so that other people in the intelligence community could look at it, you would get a whole different effect." That's exactly what happened. If you post, "This is what I think is happening," and someone says, "Well, it's very interesting that you came up with that conclusion, but it's absolutely wrong, because here's what you didn't know," or someone else enters the discussion, you then find that the things that are posted become much more accurate. You get some debate on the topic, which is exactly what we want, and it's much more real time. So it just changed the whole dynamic. That was the philosophy. John Deutch and the people Keith Hall represented, the Community Management Staff, quickly realized the value and supported rapid development of Intelink.

⁵ Steve Schanzer is the director of Intelink.

Oettinger: That was John Deutch as DCI?

DeMarines: No, John Deutch was the deputy at Defense at that time.

Oettinger: Well, that's more significant.

DeMarines: I want to point out that these are the home pages of CIA, NSA, AIA, DIA, et cetera, and that you can now enter on this highly secure network and get their opinion of what is happening (figure 22). Then, through the Internet-type services, you can send messages and debate on the topic.

This has become very effective. I wanted to use it to show how quickly things can be done (figure 23). We all sit here and say, "You can't do anything overnight. It's too hard in the military, and there's too much process involved." We had the concept in November 1993. We put forth that The MITRE Corporation, at all of those sites I showed earlier (figure 12), would be willing to help do this. So, for several million dollars we put up 19 servers and dozens of users. John Deutch declared it operationally useful. Today, there are 330 servers and 62,000 users. So, in the span of 1993 to 1997, the system has developed, and it is being broadly used in different networks.

Student: Sir, you coined the term "Massachusetts light switch phenomenon." Back in 1990 or 1991, there was this young Air Force officer—me—who was running around selling Intelink, and no one knew what it was. They thought I had the stupidest idea in the whole world. It would cost too much money. It was impossible to do. So I went to MITRE and said, "I need some help. Can you convince someone that this is a smart thing to do?" I took a bunch of MITRE people to Steve Schanzer's office. They all said, "Listen to this guy. He's got a really good idea. It's so important that we want to put money, time, and effort into it," and it happened really quickly. But without having them come in from the outside and grabbing people by the collar and saying, "This is really a smart thing to do. You need to look at it," I'd still probably be running around selling snake oil as far as a lot of people are concerned.

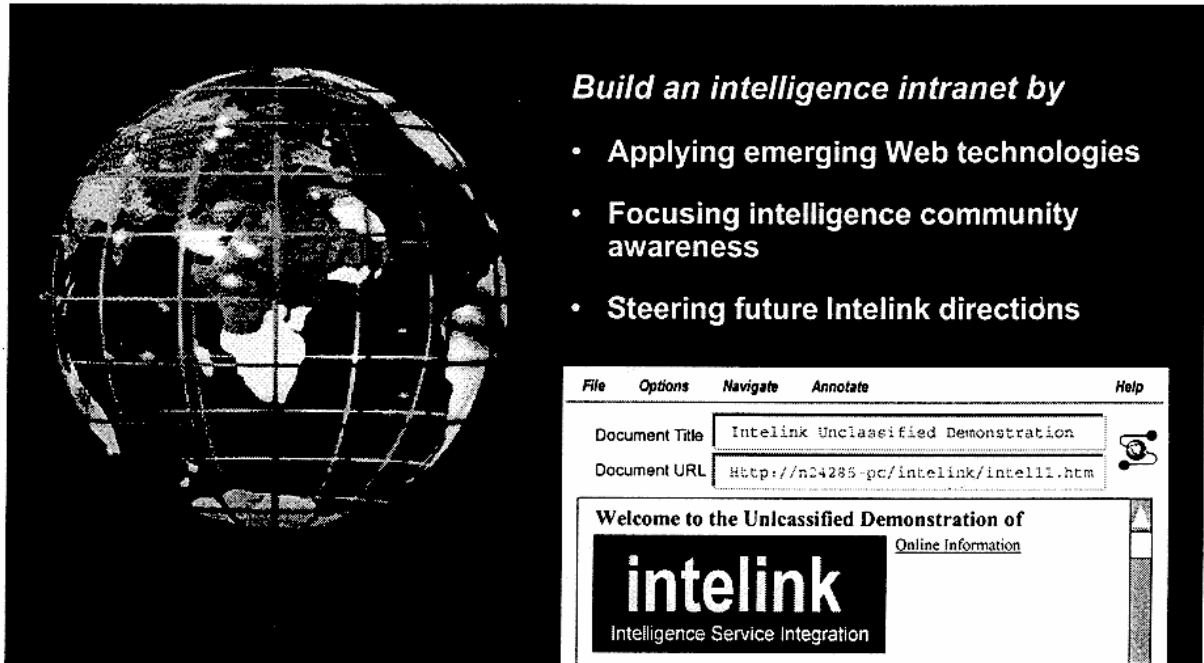


Figure 21
Intelink

DeMarines: God bless you!

Oettinger: For the record, could you explain what a Massachusetts light switch is?

Student: Oh, sure. You could have denied it, but please go ahead.

DeMarines: Sometimes, military people working within a system would have great ideas, but people tended not to listen to them because they are “insiders.” There has to be some outside source, whether it be an industry person or someone else, who would say it. Once an outsider said it, it must be right. I think we all understand that, and it’s not just the military. I term that phenomenon the “Massachusetts bathroom light syndrome.” If you notice, in most of the hotel rooms (or in any rooms, for that matter) in Massachusetts, the bathroom light switch is on the outside, in the hall. If you go to any other part of the country, you reach in and turn it on from the inside. So, this is the Massachusetts bathroom light syndrome, where you have to be on the outside to turn it on. You can’t be on

Build an intelligence intranet by

- Applying emerging Web technologies
- Focusing intelligence community awareness
- Steering future Intelink directions

the inside. It may be the only thing I’ll ever be remembered for.

Student: There are worse things!

DeMarines: I could not end this without talking a little bit about information warfare. What’s that all about? Clearly, it is about the recognition that information is the thing that makes a difference. In the Gulf War, there was ample evidence of that in precision weapons. If it makes a difference—and we are, as a country, very dependent on it—then it makes sense for us to protect our asset of information systems. It also makes sense for us to be able to do what we need to do to deny, disrupt, or destroy the information systems of an enemy.

That subject has become very active, as you know, and many are working on it (figure 24). It’s not only important to the DOD. U.S. industry is also concerned and involved. Most recently, there was a White House commission established that took a look at protection of critical infrastructure, and Tom Marsh, a retired four-star general, is

intelink

Intelligence Service Integration

Intelligence Community Intelink Testbed

[Click here for Help](#) -- [Quick link to Table of Contents](#)

Welcome to the Intelink Testbed Demonstration.

An Audio Introduction to the Intelink Testbed (3 minutes) is available.

The Intelink testbed is Sponsored by the Intelligence Systems Secretariat for the Intelligence Community. The ISS would like to thank all participant organizations for their efforts in making this a successful demonstration. A Detailed Directory of Intelink Testbed Demonstration Participants is available.

The Following Agencies, Commands, and Organizations are Co-sponsors of the Intelink Testbed Demonstration. Each symbol is "hyperlink" to that Co-Sponsor's home page.

CIA	NPC	NSA	MSIC	AIA	FSTC	DMA
USCENTCOM	USSOCOM	OPEN SOURCE	USSTRATCOM	NPIC	SPACECOM	USACOM
USPACOM	UCIRF	NAIC	ONI	DIA	USEUCOM	USSOUTHCOM

Figure 22
Intelink Testbed

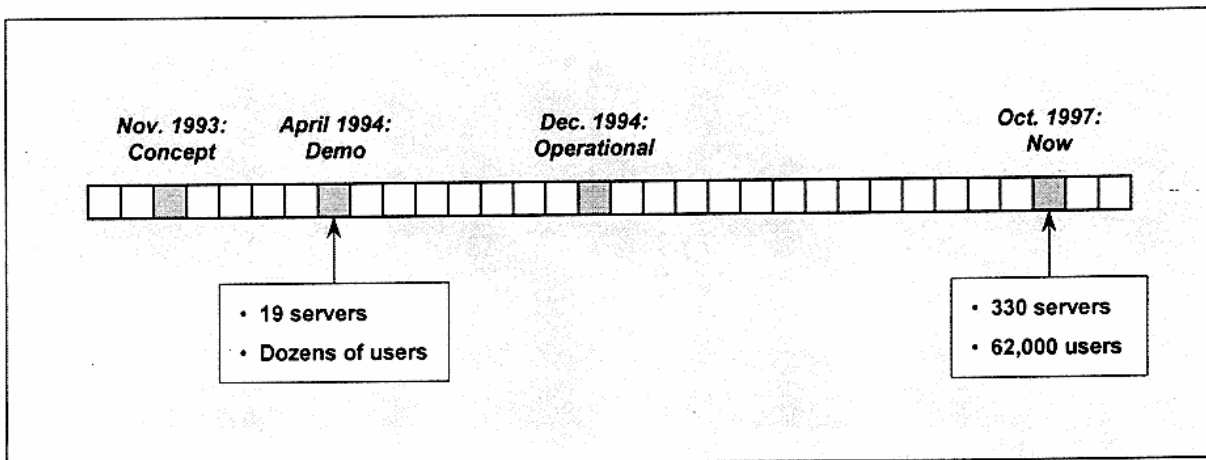


Figure 23
Intelink Timeline

Services: Air Force AFMC ESC Rome Lab Wright Lab AIA AFIWC AFCSC AMC		Army CECOM DISC4 PEOC3S } ADO ISC ARL/SLAD LIWA Navy SPAWAR/PMW161 NRAD NUWC NOSC FIWC NSG/NIWA	Agencies: CIA ISS OWTP DIA PG SC DISA DISN CISS JIEO	NSA DDI DDT DARPA ISO ITO	OSD IW A&T DMSO BMDO DTIC Joint JC2WC JWFC JPO-STC JS/J38 JS/J6K FAA
--	--	--	--	--	---

A&T	Acquisition and Technology	ISO	Information Systems Office
ADO	Army Digitization Office	ISS	[Office of] Information Systems and Services
AFCSC	Air Force Cryptographic Support Center	ITO	Information Technology Office
AFIWC	Air Force Information Warfare Center	JC2WC	Joint C ² Warfare Center
AFMC	Air Force Materiel Command	JIEO	Joint Interoperability and Engineering Organization
AIA	Air Intelligence Agency	JPO-STC	Joint Program Office—Science and Technology Center
AMC	Air Mobility Command	JS/J38	Joint Staff, Operations Directorate, Deputy Director, Current Readiness and Capabilities
ARL	Army Research Laboratory	JS/J6K	Joint Staff, Command and Control, Communications, and Computer Directorate, Information Assurance Division
BMDO	Ballistic Missile Defense Organization	JWFC	Joint Warfighting Center
CECOM	Communications Electronics Command	NOSC	Naval Ocean Systems Center
CISS	Center for Information Systems Security	NRAD	Naval Research and Development Center
DARPA	Defense Advanced Research Projects Agency	NSG	Naval Security Group
DDI	Deputy Director for Intelligence	NUWC	Naval Undersea Warfare Center
DDT	Deputy Director for Technology	PEOC3S	Program Executive Officer for C ³
DISC4	Director of Information Systems for C ⁴	SPAWAR	Systems Space and Naval Warfare Command
DISN	Defense Information Services Network		
DMSO	Defense Modeling and Simulation Office		
DTIC	Defense Technical Information Center		
ESC	Electronic Systems Center		

Figure 24
Key IW Organizations

leading this commission. It just reported last week.

Oettinger: Is the report out already?

DeMarines: It's out now.⁶ It looks at critical infrastructure, recognizing that the DOD is very highly dependent on the infrastructure. What is that infrastructure? It's transporta-

⁶ Report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*. Washington, DC: U.S. Government Printing Office, November 1997. Also available in electronic form from the commission's Web site: www.pccip.gov.

tion, telecommunications, water, gasoline, emergency services, et cetera (figure 25). If those sectors were affected in a major way, our military and our nation could be crippled. So the commission made some recommendations about how to deal with the problem and we can talk a bit about this.

First, a little background. Here is one simple way of identifying the threat (figure 26). It ranges from the hacker—the person who would play around with it in his dorm if you will—to a crook, an employee, a dissident, a criminal organization, a spy, a tactical user, a terrorist, an integrated attack, all the way to some group that wants to overthrow the government. There is a whole range of threats with which we must be concerned.

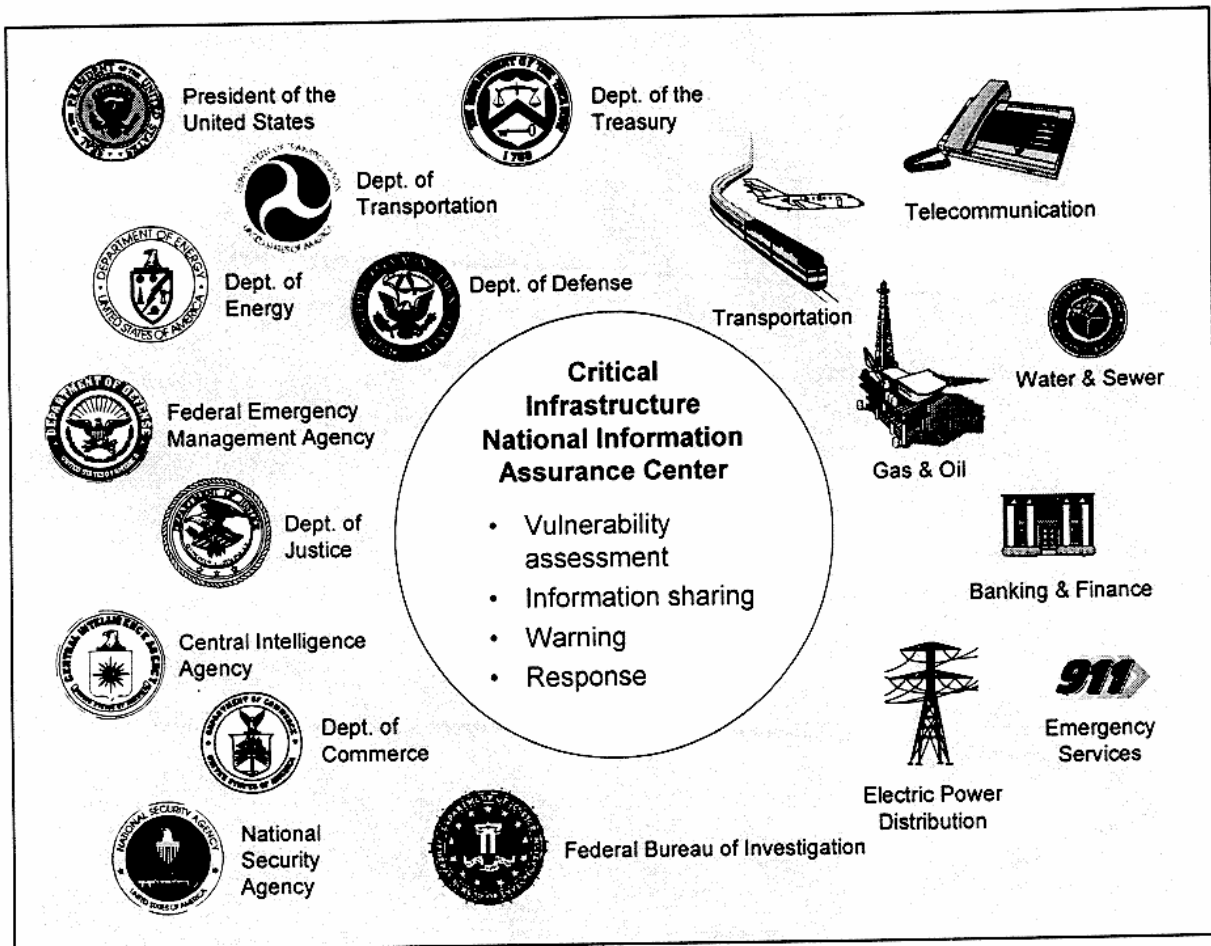


Figure 25
An Organizational Solution

The military clearly deals with preventing hackers, crooks, employees, dissidents and organized crime from messing around with its systems, and it uses good cryptological devices and other forms of protection. But problems are still occurring where a highly skilled enemy can do harm to information systems, and that's a challenge the military is now facing.

On the infrastructure side—the power, the light, the finances—they are quite open to attack, as you read every day. Hackers are quite active.

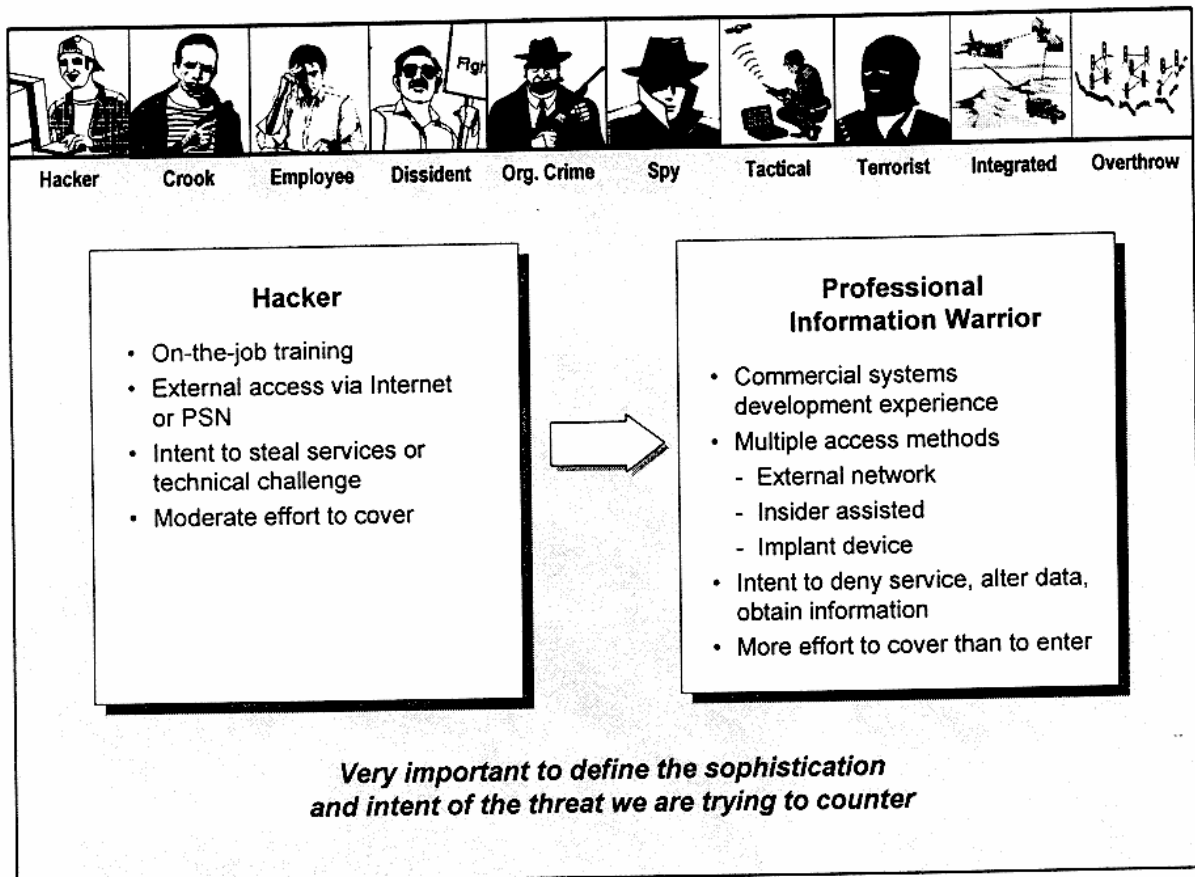
Student: What's an integrated threat? The second picture from the right?

DeMarines: This is a coordinated activity on a number of fronts, not just a single attack.

Student: An extreme case in a network is taking the primary down by destroying its transmitting tower and taking the backup down by destroying its power source. You'd go at it in two different ways. You wouldn't try to use just one method to do it. It would take two different types and styles of forces.

DeMarines: As he said, a really simple example is if you have a communication tower and it has a power source, and we say, "Well, okay, I'm going to cut off the power source." But you have a backup power source. So, one very diabolical scheme might be to force the backup source to come on at odd times, to cause it to run it out of gas. It would be an integrated attack.

So, what we must address is how to deal with the infrastructure industries. Clearly the



© 1997 The MITRE Corporation. All Rights Reserved.

Figure 26
IW Threat

military knows they have the problem of dealing with protection and the denial or the destruction of the enemies' information systems. There is a difference between the amateurs on the left of the slide and the highly professional people on the right.

You all may be too young to know what a Bear bomber is. I know because I've been around a lot longer. If there were a Bear bomber threat against the Western countries, would there be any doubt in your mind that our military must deal with it? No. You would say that's exactly why we built the SAGE (Semi-Automatic Ground Environment) system; that's why we have fighter interceptors. Our intelligence community would certainly have a full set of activities to determine the order of battle, technical characteristics, mission profiles, indications and warning (figure 27).

What do you do when you have an IW threat? Well, you might do somewhat the same thing, except now with different terms (figure 28). The order of battle includes nation state IW threats, and technical characteristics including malicious software code. Is the military responsible for the infrastructure? Absolutely not, but is it important to the country for the military to know that that threat is there? Absolutely yes. So, the issue must be one that is dealt with jointly.

Student: That is a very interesting question, but I think the emphasis to keep putting it into the defense arena is probably natural, but not necessarily accurate. Certainly, attempts to overthrow or disable the United States by disrupting our currency by forgery is not anything that the Defense Department really has a lot to do with, unless you start talking

<p>Order of Battle</p> <ul style="list-style-type: none"> • Number of aircraft • Types and variants • Subordination • Basing • Runway lengths • Dispersal bases • Weapons storage • Support infrastructure 	<p>Technical Characteristics</p> <ul style="list-style-type: none"> • Range • Payload • Max speed • Max altitude • Crew size • Defensive measures • Delivery accuracy 	<p>Observables</p> <ul style="list-style-type: none"> • Radar cross section • Communications • Navigation • Beacons • Altimeter • Visual cues • ECM
<p>Mission Profiles</p> <ul style="list-style-type: none"> • Ingress and egress routes • Weapon release altitude • Refueling points • Altitude profiles • Defensive tactics • Targets • Phasing of attack • Command and control • Return basing 	<p>Indications and Warnings</p> <ul style="list-style-type: none"> • Flight standdowns • Activation messages • Crew recall • Weapon status • Forward basing 	<p>Other Areas</p> <ul style="list-style-type: none"> • Readiness assessment – Pilot and crew proficiency – Maintenance and reliability – Exercise tempo • Research and development • Concepts and doctrine • Identification of vulnerabilities

ECM = electronic countermeasures

Figure 27

Defense Intelligence Responsibilities — Bomber Threat

about interdicting the means of transporting that currency to the United States. There's a whole government organization that does that, the Treasury Department, and all the rest of that. Have we, as a nation, settled on the Defense Department as the people who are supposed to be doing this?

DeMarines: Not at all. In fact, if you talk to Boston Edison and say, "Do you want the government to impose criteria upon you to protect the power source from hacker attack?" what will they say? "No way. That's a cost. That would destroy the competitive position I'm in. I don't want you to do that." But if there is a real smoking gun, if it's obvious that we have a problem, then we'd see the energy build up to take action. You'll find that people here prefer to run businesses with little oversight, yet it's very important for the country as a whole to have some sort of protection.

The interesting thing about this technically is that the dependence on information systems has skyrocketed. A long time ago we used to run power systems in this country with their own integrated telecommunications systems. What do we do now? We tend to run everything through satellites, so there are a single points of failure—the satellites. If you want to control trains, you go to Orlando, Florida, because it has a major control over train switches in the United States. If you want to do something to the other systems, that's also possible. Why? Because we try to centralize, to make the system more efficient, use digital processing techniques, and what is the effect of this? It makes them much more vulnerable. Air traffic control can be run on GPS. That's satellite based. You don't use data links. It's a very central target. So the trend line is to make everything more efficient by making it more centralized; more centralized makes it more risky; more risky makes it more likely that disaster can occur.

<p>Order of Battle</p> <ul style="list-style-type: none"> • Nation state IW threats • Transnational IW threats • Insider IW threats • Access locations • Technology and tool suppliers • Telecom and network topologies 	<p>Technical Characteristics</p> <ul style="list-style-type: none"> • Denial of service • Session stealing • Information theft • Spoofing • Black hole and ping attack • Malicious code • Encryption countermeasures 	<p>Observables</p> <ul style="list-style-type: none"> • Penetration attempts • Failed logons • Honey pot traps • Active probes • Varied results from repetitive processes • Encryption and traffic patterns
<p>Mission Profiles</p> <ul style="list-style-type: none"> • Internet access • Telecommunications access • Trojan horse software • Implanted devices • Insider assisted • Masking tactics • Precursor viruses 	<p>Indications and Warnings</p> <ul style="list-style-type: none"> • Software verification failures • Increased CERT reporting • Protocol analysis and weaknesses • Network mappers • "Coincidental" failures • Changes in network configuration • Encrypted traffic volume 	<p>Other Areas</p> <ul style="list-style-type: none"> • Bulletin boards • Seminars and symposia • Tool R&D • Technical papers • Recruitment of professionals • "Cooperative" developments

CERT = combined environmental reliability testing

Figure 28

Defense Intelligence Responsibilities— IW Threat

When you come to MITRE (I believe there is a scheduled trip that some of you are going on), you'll see what we call an IW War Room, where we walk through each of these infrastructure industries and point out the problems that seem to be facing them. The reason for bringing up information warfare is that this is where I see MITRE affecting things next. We're working at DOD and in the FAA, but this problem is facing the nation. It is one in which we have strong beliefs and heavy investment.

My last chart sums up MITRE and our technical competencies (figure 29).

Oettinger: Questions?

DeMarines: You asked when the White House report on the Gulf War activity will be coming out. It's due out next week. We've seen it around, and it will say very nice things about the MITRE report.

<p>MITRE: Solutions that Make a Difference:</p> <ul style="list-style-type: none"> • System-of-systems integration and interoperability • Technical requirements and specifications • Systems research and development • Test planning and evaluation • Source selection and acquisition management • Analysis • Concept development • Field integration planning and support • System architecture • Supportability and sustainment

Figure 29
MITRE Capabilities

Student: One other place to find stuff on the Presidential commission is their World Wide Web site. The address is www.pccip.gov. General Marsh gave a speech last week, and overviewed the likely conclusions and recommendations.

DeMarines: He recommended that there be a public-private organization created to wrestle with this, which is meeting a lot of resistance. Some of this resistance is kind of interesting. EDS (Electronic Data Systems), the company that does outsourcing for data processing said, "If the government knows there's a problem here, just tell us what they want to have fixed, send us a check, and we'll fix it."

Student: How do you promote people or organize your company and your employees to be innovative as a derivation of the government, especially DOD? If you have the same sort of structure I'm familiar with, innovation is not inherent in its character.

DeMarines: That's a really interesting problem. We do it by having technical centers. We do it by making research money available to people to be innovative. As I said, we work on the front end of the problems, and you can see the importance of innovation. I think innovation is a cultural thing. The people who started MITRE were the ones who invented rotating memory, as well as pioneering other computer developments. You need to be careful and promote the right people. If everybody knows it's important to the company, then it becomes important to each individual. It's the sort of a thing where leadership makes a difference.

We do lots of things to promote innovation. We have frequent sessions where people interact on technical topics, or on subjects of cross integration. We may have three or four projects working on tactical missile defense. We will bring them together and debate the issues, and make sure we do something collaborative. It's a competitive thing among the groups to make sure the end product works. I don't know if that answers your question about innovation, but I think you will read that it's a cultural thing that determines the style of the company.

Student: I'd like to go back to one of your last points about the increasing move to centralize, and that while it gives more efficient control you also get greater vulnerability. Going back to something earlier in the presentation about digitizing and using GPS and so on, do you see that that opens up new opportunities or different opportunities? Say that a plane is shot down, but it's not totally destroyed; is there a risk then that not only your commander would know where all of your Bradleys or M1s are, but now the enemy would also have that ability to see exactly where they are?

DeMarines: Very much. We took note of this mistake in the infrastructure industry review. The military wants to continue efficiencies and accuracies, and use data processing, and are more interested in the function—the accuracy—than in the protection so that they can prove the worthiness of the concept, and they do exactly what you said. They buy into risks that are not well thought through. When you're trying to get something done with a relatively few dollars, you're not going to pay as much attention as you might have in the past to protection, or thinking through the issue completely. That is a problem facing our military today. We see it time and time again. Task Force XXI was an experiment, but will the Army make the necessary investment to protect the system from IW attack?

Student: But that would be a risk that you would definitely try to alert them to.

DeMarines: Yes.

Student: Going back to the topic of the AWACS, how much do you commit in the sale to the Japanese self defense force? Are you just selling the hardware, or are you also selling the software to coordinate the AWACS of the Japanese self defense force with ours?

DeMarines: The Japanese are buying directly from industry—Boeing, and Westinghouse for the radars. Our Defense Department will permit everything to be given to them, with some exceptions when it comes to

electronic warfare or cryptology. In fact, the Japanese AWACS will be a superior AWACS, in that it will fly in a modern airplane (the 767). It will be flying higher, longer, and it will have improvements in the radar that comes with the last version.

Student: So, how do you assess interoperability between the Japanese AWACS and the U.S. AWACS? Do they have technical interoperability?

DeMarines: Yes, there should be interoperability so that when the U.S. and the Japanese fight in a combined way, they can share data. That will be part of the structured deal on the system.

Student: I have a question related to information warfare and vulnerability. A lot of people talk about an electronic Pearl Harbor—and this type of hype about these dangers, I guess, is common in some circles—while other people would argue these information systems have also a lot of redundancies built in, even more so. So I just wanted to get your view and assessment.

DeMarines: I wish it were so—that there were redundancies. We find some interesting things about air traffic control systems. Our air traffic control system is actually a set of systems, and they handle such emergencies as, “If the radar goes out, what will the pilot do? If the VOR goes out, what will the pilot do?” They have backups where it comes down to radio communication. So they have a lot of redundancy in place, not by any thought process, but because bureaucracy never throws anything away. We just kind of keep things, where a business-oriented organization will dump something old to put something new and more efficient in, even though they’re buying more risk. I wish we had more backups for things, but we don’t. Maybe I can give you a couple of examples.

We had a West Coast power outage of some major proportion in this last year. How did that occur? It occurred because they put a digital control system in, controlled by computers, and when a certain set of events caused a failure, they had to take generating power off line to protect the generator, which

caused a ripple effect. It wouldn’t have occurred in the way their prior system was configured, because of checks and balances, and the interaction with people to make such decisions. But because it’s computer oriented, the effect was felt from Washington to California. So, it shows the dependency, and the fact that more is needed to provide adequate control.

Student: Along that same line, using the West Coast power failure as an example, most of these cascading types of events and outages have been on the order of hours or, at the most, a couple of days. Even the Internet worm was cleaned up within a couple of days. Has anybody systematically studied how to use this as warfare to sustain an effect over a long period? You don’t generally paralyze a country with a couple of days’ disruption. Has anybody studied the sustainability of effects against an infrastructure?

DeMarines: Excellent question. People tend to believe that if you’re having a computer attack you shut down and reboot the computer and bring it back up and get it back to work. Of course, that’s not true. We were paid by the Marsh commission to examine a single instance where we could show a sustained effect, and we picked the New York City power outage. Could we sustain a cyber attack that would have a lasting effect? Through our dialogue with clever engineers, they worked out something that would affect the system for weeks. Our people figured out what they would do when certain things would happen, how to take advantage of their rote processes to recover from things and accelerate the damage.

Oettinger: Did you do that with the cooperation of the power company?

DeMarines: We went down to the power company, and said, “Is this fairly accurate? We don’t want to be beating you up.” The representative said, “Oh, yes. We know about that, and we know about 100 other such things.”

Student: There was a study done by some officers at Air Command Staff College about

three or four years ago where they found out that in almost every case where they looked at different ways to take down power grids, none of them had consequences good enough to make it worthwhile. The trouble it was going to cause later on to them in controlling the population—the unintended consequences of the population going to the wrong places after the power went out—all turned out to be so bad that it wasn't advisable for them to take the power out. It was better to leave it there so that the population wouldn't move around so they'd have problems elsewhere.

Student: Regarding the information warfare discussions and studies that you're involved in, do they, in your opinion, focus unnecessarily on the cyber attacks? People can talk about how they've got this great cyber bug that can go in there and do this stuff, whereas one van full of nitrogen explosives can take out that Orlando center, and you're not going to have some smart people come in tomorrow and figure out how to get around the bug. It's now a physical construction issue.

DeMarines: I don't know what the answer is, but the commission addressed two issues. One dealt with cyber attack, and one with conventional attack. The conventional aspect was handled by the FBI. Of the two, in my view, cyber attack is more interesting. You do it from remote locations and that diminishes the risk of exposure. It has a certain gamesmanship about it, and, therefore, it becomes more fascinating. But, you're right, a satchel of explosives ...

Student: But there's an overlap there. You talk about cyber, cyber, cyber, but that same site can be subject to something that's not even a hostile act—a natural disaster, for example.

DeMarines: You're absolutely right.

Student: You talked about integrated attacks before. When I think about cyber attacks, I rarely think about taking things out. I think about how to take advantage of them so you can monitor them. If you could find a place where you could get into certain nodes in a network and collect intelligence from those,

then it would behoove you subtly to force more traffic to go through those, hopefully without being caught for a very long time. That's of more value than taking out the network.

DeMarines: Much more value. In fact, if an enemy air defense network has the big picture of the air scenario, wouldn't it be nice to put a few phony tracks of F-15s in there? Of course, there would be no real F-15s, but it might cause them to divert their attack. That's a powerful strategy.

Student: I think what he is saying is that it would be better because if you had the entire air picture, you wouldn't have to send your airplanes in to find it out. You would know where their airplanes were. You could just go after them there.

DeMarines: That's a subject that used to be called C³CM—C³ countermeasures.

Student: There is obviously a tension between learning and when you want to have an effect. We faced this about taking out potential sources of intelligence information, depending on your other means. Certain opponents might not have an air force to fight us with; therefore, disrupting our Air Force through cyber attack might be much more useful than just learning and taking advantage of it.

DeMarines: The topic is now being raised in testimony on the Hill, where such people as Jack Gansler⁷ call it an "asymmetric attack." It recognizes that enemies elect not to fight us gun for gun, airplane for airplane, tank for tank. They'll do other things, such as mounting a cyber or terrorist attack and have the same effect—taking hostages or whatever it might be—and avoiding the problem of competing militarily. It just doesn't seem to make any sense. An asymmetric attack makes sense, whether it's nuclear, chemical, biological, or cyber.

⁷ Jack Gansler, formerly director of corporate planning at TASC, was confirmed as assistant secretary of defense, acquisition and technology on November 5, 1997.

Oettinger: It strikes me as an open question as to whether the ability to learn the details isn't very difficult to attain. The intelligence effort required to mount a sustained, effective, controllable attack is not negligible.

DeMarines: Not at all.

Oettinger: What strikes me as very curious about these debates is that when you talk to people about doing things offensively, they point out about how hard it is to get into damn' near anybody else's knickers, and yet, at the same time, how easy it is for somebody to get into ours. The asymmetry of that assessment worries me, because if it's that hard for us to get to somebody else, well then, it can't be quite that easy to get to us. The resolution comes out of the involvement in the details of what you need to know to be effective, as opposed to being random.

Student: Exactly. On the slides you showed of what we had to know to assess a Soviet bombing attack coming versus the information to know that a cyber attack is coming, or, to flip it around, to launch a cyber attack, you had maybe 30 or 40 categories of information (figures 27 and 28). Our development of the data sets to fill in those sets of information seems fairly low. I'm an intelligence officer by background, but I did Soviet bomber analysis, so my capability to fill in those sets for cyber attacks is pretty limited. So it's going to take us a long time, but, hopefully, it will take our opponents a long time too.

DeMarines: I guess that's a fair point. I think we know a little bit about the offensive side, but, obviously, we don't talk about that.

Oettinger: Historically, one wonders about effectiveness. A lot of the literature, talk, and testimony about information warfare today is reminiscent of the heyday of the Army air corps and whatever air enthusiasts talked about strategic bombing. Every post mortem on strategic bombing suggests that it didn't accomplish what the enthusiasts claimed it accomplished. Whether it's ball bearings, or Iraqi command and control, or Vietnamese

lines of supply, after the fact, all the bombing, while it may have been high in casualties and one thing or another, didn't manage to do a hell of a lot from a strategic point of view. Historical reasoning like that is dangerous, but so is shooting from the hip on "the sky is falling," and I guess my concern is that we haven't really managed to net this out and to have a sensible assessment of the dangers.

DeMarines: That's true, but we haven't really thought it through. We get caught so easily. Everybody knows they're putting GPS receivers on conventional munitions to make every bomb a precision delivery weapon. We also know that a jamming transmitter about the size of this cup would be effective in jamming GPS for many square miles. In fact, the Russians are selling jammers on the open market; they cost about \$1,000. What would happen if you released these bombs, and these guys have screwed up the GPS? We would render a huge number of warheads unusable. So we have this tendency to jump into something that is technically and functionally achievable, without thinking through the consequences.

Student: I think that gets into what someone said about the senility of weapons systems, and that as technology advances and changes faster and faster, we're getting to the point where you get to use a trick once and that's it. Is it going to be worth the amount of money you spend to use that trick against one opponent once? Maybe it's not going to do you any good anyhow.

DeMarines: Let me tell you, if a trick is that fragile, it will never be used.

Student: There is a discussion now that maybe stealth aircraft was a one- or two-trick weapons system, but its value is now starting to go down.

Student: You mentioned as one of the strengths of your corporation that you have the ability and the finances to hire experts who might be not affordable by ministries, for example. Do these persons get into contact with high security material as well? Whose responsibility is it to make them un-

dergo certain kinds of security checks? Is it the government, or do you have a kind of department within your corporation?

DeMarines: It's a very big business for us to make sure that we hire people who, first of all, can get at least a Secret clearance through DOD. The contracts we sign with DOD and others require that levels of clearance be in position. That's a very hard thing to comply with, but it is absolutely required. We have the Defense Security Service (DSS), which polices this for the U.S. In our company, we don't clear the people for classification. That's the job of the DSS. It takes a long time to get a clearance. Six months is not unusual.

Student: That's the problem in Germany as well. It's very time consuming. Because you are interested in getting people as soon and as quickly as possible, I would think that there is a certain tension, because it takes time.

DeMarines: There's a big cost of people sitting there for six months, waiting for the opportunity to do some work.

Student: In hiring people, you probably have to be kind of careful about how many former government and military people are mixed in at MITRE.

DeMarines: We have policies. We had a favorite general at Hanscom once who said that if he wanted another colonel, he'd hire another colonel. When he hires The MITRE Corporation, he wants qualified engineers who have a sense of what the military is all about. But we find that is going too far. About 5 percent of our staff is retired military, because we find that some of the former military people come not only with military knowledge, but also with highly technical skills that are very useful for us. In such cases, we will hire them as long as there is no conflict of interest. We will never use them in the venue from which they came. A hire from the Air Force might go work for the FAA or something like that.

It's something we look at very closely, because you can understand the kind of position we'd be put in. We work every day with the military, and if people want to retire, they

say, "How about hiring me?" It is our company policy to say, "I'm sorry, it is our policy not to hire from the customer." You find a far different policy in other companies. If you went to an SAIC or a BDM and asked the same question, you'd get a very different answer. But MITRE can't afford it.

Student: To continue this, what is your culture about employees leaving the company and all the knowledge they take with them?

DeMarines: It's the same practice. MITRE security services will interview them on leaving, and review their continued obligation to safeguard proprietary and classified information. They will go through a formal process to remind them what the responsibilities are of protecting data forever.

Student: You can protect data, but surely you can't keep them from using knowledge about systems or methods.

DeMarines: I sure hope so.

Student: There are lots of leaks.

DeMarines: I suppose that's possible.

Student: Can't someone not sign an agreement and emigrate?

Oettinger: Think about it. If you look at public knowledge about World War II cryptography, it took 30 years for significant leaks to take place. The books on Ultra and so on did not appear for a long time. There were a lot of people walking around with that knowledge, so it's not an impossible task. Now, if you want a counterexample, you only have to look at the newspapers, at the Ames case and several others, where people walked off and, for whatever reason, sold their knowledge. So I'm not saying it is inevitable, but it certainly can happen that people keep their mouths shut. Many people have done so for a long, long time about very secret topics.

Student: They actually should just hire people who aren't likely by character to do that.

Apart from that, you really haven't got a safeguard. An agreement could be breached.

DeMarines: We have an organization in this country, the American Civil Liberties Union, that says it would be a discriminatory practice to make a prejudgment about the character of a person. We would not live for a day if we did that.

Student: I'm not recommending direct discrimination, but indirect discrimination, whereby you institute certain procedures or certain criteria which indirectly will eliminate certain types of people.

DeMarines: We do. We will not hire people who have a criminal record.

Student: Even certain personality types I'm sure can be related ...

DeMarines: No, that's not possible.

Student: So, what is the safeguard, apart from a piece of paper, to stop someone—maybe a disgruntled employee—from talking out of turn?

Oettinger: Ultimately, there is none. It's like assassination. If I want to kill the President and I'm suicidal enough, I can do it. There are some things that are unavoidable. That's what I'm telling you. Empirically the answer to your question is that by and large people do not blab, but some do. So, there's an unavoidable risk.

Student: The reason why I'm asking is that your own people have the most knowledge, and some possible opponent across the world is not going to have that intimate knowledge. This is a weak link in the chain, and yet no one looks at this side of it. Everyone's consumed with the other side.

Oettinger: Think of Klaus Fuchs, or think of Burgess and Maclean. History is full of major cases of people with critical knowledge walking off and selling it or giving it for free for illogical, venial, psychological, or whatever reasons. However, I also cite a few examples on the record of a period of 30 years

where no one out of thousands said a thing. So, I think that is about all one can do or one can say.

Student: I think maybe you ought to look at the market. I don't know much about World War II, but there must have been a market after the war was over for that sort of knowledge, and I assume there's a market now.

DeMarines: There was a market.

Oettinger: There were plenty of markets.

Student: I think that within the IW literature the relative importance of the human underpinnings of information infrastructure is underemphasized. In terms of creating and filling in those databases, it's a lot easier to do it if you can corrupt an individual or two than to go in and try to do it remotely, electronically.

Oettinger: Of course. That has always been true. The cheapest way of getting access to information is to buy somebody.

Student: Not just cheapest; I think it's probably most effective.

Student: There is more of a market now, I would imagine, for highly developed computer expertise because there are more global mechanisms for the exchange of information and validation of your skills than there were post-World War II. Cryptological knowledge has always been at a premium. I'll have to admit that.

Oettinger: You made a very good point earlier that the private sector gets a tad careless and so does the military. I understand that if you put all your eggs in one basket in areas of old technology, you run a high risk. That is equally true in the cyber world. I am mindful of the first days when I worked with banks many years ago, it was their practice that everybody had to take a vacation: two weeks at least. It was an iron-clad rule. No one was permitted to work the year around. The reason was very simple: it's very hard to sustain an embezzlement if you're away from it. Most embezzlements are highly time sen-

sitive. So you take precautions. You force your people to take vacations: every teller, every vice president, everybody.

Student: Somebody else has to do your job for two weeks to give them a chance to discover it.

Oettinger: That's right. I would run a critical software shop that way, too. It buys you two things. It buys you backup knowledge, and it buys you somebody who will discover

the scam or increase your chance of doing it. So, you're right. People precautions are absolutely essential. They're at the heart of everything, and high tech hasn't changed that one bit, or one byte. Sorry.

On that note, before we get really out of control, I want to thank you very, very much and present you with this small token of our large appreciation. Thank you, Vic.

DeMarines: Thank you very much.



INCSEMINARF1997



ISBN-1-879716-54-2