INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

C^3I and the National Military Command System
Lee Paschall

Guest Presentations, Spring 1980
William E. Colby; Bobby R. Inman; William Odom; Lionel Olmer; Lee Paschall; Robert Rosenberg; Raymond Tate; A. K. Wolgast

December 1980

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
I-80-6

C^3I AND THE NATIONAL MILITARY COMMAND SYSTEM

Lee Paschall

**Consultant; Formerly Director,
Defense Communications Agency and Manager,
National Communications System**

Before retiring from the military General Paschall directed both the Defense Communications Agency and the National Communications System. That mammoth management job gives him a firsthand basis for judging how C^3I is applied in daily reality — political, operational, technical, human. Such a system is ordinarily taken for granted — or cursed — by those without background or experience. The practical experience of its chief is a unique view.

I was asked to talk about some of the practical realities of life in Washington concerning command, control and communication systems, and I'm going to begin by giving you what I describe as the fundamentals. I do that not to insult your intelligence but rather so that you will know where I start from and what I place emphasis on. To me, a command and control system consists of an organized arrangement of sensors, communications and command centers. Whether you start with a data entry device, or a sophisticated satellite sensor, or communications, which are probably the critical link of any command and control system, it is at the command centers that all the information comes together, is processed and decisions are made.

There are two other elements to a command and control system that are far too often omitted; and generally when they're omitted you have a disaster on your hands. They are people and procedures. Very often we implement the procedures in the form of computer programs or in displays, or in checklists of actions to be taken under certain circumstances. You may have heard that the World Wide Military Command and Control System

is a failure because of its Honeywell computers. There are a number of people who equate command and control with computers. One of the first things we should collectively understand is that computers are aids. They may assist the executive in making his decision. They may record, file, process or display information; but they are only an aid to the people who are making the decision and then in communicating that decision to whatever force is taking the action.

What, then, *is* C^3I? *Is* there a C^3I "system?" It's a current sex symbol in Washington, of course. The technologies being used in the technical collection of intelligence and those that are used in the command, control and communications process are merging. (They're all, incidentally, elements that are used in the command and control process.) What C^3I is is a convenient way to manage a collection of similar items and elements — that's really all it means to me. At the beginning I thought that was desirable, and I've come to believe it's essential, for reasons I'll give you later.

So for me C^3I is not a system; and I think it's misleading to think of it as a system. Rather, it's a grouping of like elements for management purposes. There are people who will debate this with me.

The next thing I would say that's fundamental to understanding C^3I, particularly in dealing with C^3I justification, acquisition and management, is to know who you're talking to — know your audience. If he is a technocrat you can talk to him in terms of a "C^3 system," an aggregate of technical sensors, communications, command centers, people, procedures all tied together to operate in accord with some central directive authority. And the technocrat is comfortable with the idea of a "system" like that. If, on the other hand, you're talking to a manager, the Gerry Dinneens of the world, then today you'd best talk about C^3I, because you're talking about a program — a chunk of the Department of Defense budget. If you're talking to an operator, the Bill Odoms of the world, then you're talking about a process, a command and control process, which is facilitated by the system, all of which is financed by a C^3I program. People in Washington, military people very often and technocrats most often of all, make the mistake of talking to people as though everybody were a technocrat and everybody were thinking command and control system. The operators, who think in terms of the command and control process, will die on the ramparts of definitional war — they will define and fight and quarrel about roles and missions until the technocrat is thoroughly confused; and the reason is that they have a differing perspective on what it is you're talking about when you say command and control. So I'd urge that you always make command and control the modifier, whether it's a system or a program or a process; and that will facilitate communicating with people who deal with command and control today.

I'm not sure that doesn't also apply in management systems. Since I've retired I've done some consulting and I find some of the same inhibitions and definitional problems that we still see in the military. What are the differences I see between a command and control system and a management system? Well, first of all, a command and control system requires near-real-time decision making. The whole purpose of a command and control system is to gather information into one place and array it in such a way that the commander or the decision maker can make a rapid decision. This applies to more than military systems; I submit to you that Three Mile Island, for example, is almost a classic case of a command and control system that went astray, and tends to illustrate the importance of three things that you must ensure in military systems. First, your people must be

trained — overtrained if possible. Next, your procedures must be sound and exercised frequently. Third, your sensors must be believable, and tailored to the amount of information people can accept. Three Mile Island was almost a classic case of what I call "information overload" — all the bells and alarms and lights in the world rang, confusion reigned supreme and decision making, the real-time decision making that should have taken place, did not occur.

One further caution: whether it's a command and control system or a management information system which simply displays from a point-of-sale cash register in the store and makes an adjustment in inventory and billing when the keys are pushed, don't leave it just to the technocrat. If you do, you will get a very exotic system that may or may not do what you want. Incidentally, I speak as a technocrat — those are my biases, and you should know that. But the fact remains that if the user cannot define his information needs and make them understandable to the system designer (and that's not always easy to do), you're in trouble instantly. Defining information needs is the first and toughest task of building an automated system, whether it's a military command and control system or a simple point-of-sale management information system in a department store. And it's not often done very well.

Oettinger. Do you think it's doable at all? Maybe it's a will-o'-the-wisp, and one has to learn to live with designing things that are flexible enough so they can work in situations where the needs have not been clearly defined. Or do you think that's all nonsense?

Paschall. I think it's very unlikely that you will ever, on the first attempt, define the information needs with precision and design the system to satisfy that defined need. I think you will, through iteration and reiteration, educate the user and the system designer as to what the system really ought to be doing — rather than what the user thought it should be doing, or what the system designer thought the user wanted. One of the management problems associated with command and control is that you build something, and you see other things you can do with it or other things you want done with it, and it tends to evolve over time, through iteration and reiteration and through block changes, if you will, in the system.

Oettinger. I feel more comfortable with what you said just now, because I could misread your earlier statement as saying that needs are definable, and can be defined, and stay put if only one puts one's mind to it instead of neglecting it. What I hear you say now is somewhat different.

Paschall. I emphasize this because all too often a far too casual attempt is made to define information needs right on the front end. I hope people will sit down and honestly try to do a good job of it, but without expecting that they're going to reach the ultimate system in one jump. They won't — at least I've never seen one yet that did.

Now there are others who say that command and control systems are really just a premium slice of management — the upper levels of management — and there are some who'll tell you there's no difference between a command and control system and a management system. I don't agree. My distinction is near-real-time decision making, which is not just the province of the military operations community, but also has application in

other areas. I'm sure you'll develop your own viewpoint by the time you finish this seminar as to how much difference there is, and indeed, in your minds, what that difference is.

Now, having gotten through the fundamentals, let's talk about some management problems. Paschall's Law is that the management difficulty associated with acquiring a command and control system is proportional to the system's complexity. Now, I don't know in what proportion. I've been involved in some programs where I thought it was directly proportional, and in others I thought it was exponential. But I think there are two groupings you can make.

At one extreme is the closed-loop system, where there is a single customer, or a single user. And those are relatively easy. SAGE (Semi-Automatic Ground Environment) was an air defense system built in the late 1950s; it was then at the forefront of the state-of-the-art. Radars put the radar data into tracks, sent them to a computer, the computer arrayed them, removed the extraneous ones and the duplicates, presented that for display in front of a weapons director, and recommended which fighter airplane should be sent up to intercept the bomber stream. Then it communicated with the airplane, giving it heading, altitude, speed, all those kinds of things. In other words it was a closed-loop system — everything was tightly fed back around, and it was serving a single customer and a single mission that could be rather easily defined — the air defense fighter-interceptor kind of job. It was the first time, I believe, that data circuits were connected to computers in real time, and the first time that digital computers had calculated vectors for fighters; and it was a howling success. It went through seven or eight generational changes as we learned more in the process of the thing, but it was a success. And at the time it was authorized and approved and work began on it, the Air Force regarded it with great fear and trepidation, because they just didn't think anything that complex could be designed. The fact that it was complex, and was designed, and was successfully implemented without much in the way of a cost overrun and without much schedule slippage, may have led us down the primrose path — because after that we were willing to try anything.

At the other extreme, which may be my exponential proportion, are the hardest ones — those very large, unbounded systems with multiple users involved. And that seems to be all we deal with today. What is an unbounded system? It's one that seeks at the one extreme to provide command and control of a chief petty officer on a landing craft on the gravel outside Beirut, one of those people whose job it was to remove the American citizens who were in Beirut at the height of that civil war over there. It ranges from that extreme to execution of the whole of strategic air command in response to a nuclear attack by the Soviet Union — and, literally, everything in between. From the small crisis involving one boat and one chief petty officer all the way to the holocaust of nuclear war. It is not bounded within any single military service, or within a specific piece of geography like the United States. It is not quantifiable, in the sense of being able to say how many crises, what's next, how many troops will I have on the scene, and where will the nearest ship be — it's open-ended and everybody's involved in it. The Army, the Navy, the Air Force, the Marines, the State Department, other civil departments of government, the President, the Congress all get interested. That kind of system is very, very hard indeed. There is no single customer, there is no closed-loop task that you can quantify and design to; and those systems are inordinately difficult. They are the ones I dealt with for four years and the ones from which I'm going to draw most of my lessons learned.

I think it's important for you to know about two of these large, unbounded multiple-user systems used nationally today. I've alluded to one of them — the Worldwide Military Command and Control System (WWMCCS), linking the National Command Authority — the President, Secretary of Defense and their successors, advised by the Joint Chiefs of Staff, their military advisors, with facilities in Washington called the National Military Command Center and two alternates, one airborne for survival and the other underground in Maryland to provide some limited survivability — with the commanders of the operating forces of the military services. It may be used for the purposes I've described, everything from evacuating citizens from Beirut, to withdrawal of all the forces from Saigon, to exercising the new rapid deployment force. WWMCCS consists of computers in selected command centers, extensive communications, procedures, and people.

The other large, unbounded multiple-user system is the National Communications System. A word about the NCS, because it illustrates a couple of things I think will be useful. The National Communications System emerged from the 1962 Cuba experience when President Kennedy tried to consult our Latin American neighbors. He urged the inter-American affairs group to consult their governments, and when all the ambassadors from the Latin American countries tried to do that, the communications problems they experienced were absolutely appalling. Finally, one country had to abstain; another country, whose ambassador couldn't understand over the telephone line what his government was saying to him, nevertheless decided to vote for the blockade, and earned President Kennedy's gratitude thenceforth. Based on that, President Kennedy said we must organize our national communications better, so an executive order was issued. It provided for something called the National Communications System, which was to be a "unified" system. It was to be put together by connecting, or interconnecting, or unifying, all the communication systems of those departments of government which dealt with or could contribute to national security activities.

One of the first interesting things, I suppose, to learn about government is what happened to the word "unified." There was a ten-year debate about what it meant. Did it actually mean a single system, which meant that the Department of Defense and the State Department and the GSA and NASA and all the other contributing agencies would be served by a single system? There were those who felt that way. There were others who felt that what that really meant was that they should all be connected together, so that if the President wanted to talk to Colombia and NASA had a tracking station in Colombia, why, he could use that link through the NCS management structure. All through that ten-year debate, many people moaned and groaned and wailed about what was meant by "unified." I draw two conclusions from that — these are my biases again. First, it's very difficult in a Presidential executive order to get completely unambiguous wording so that people can't argue over what was the intent, what was the meaning. Second, it may not even be wise to write an executive order that's completely unambiguous, so that there is no debate — it sort of forecloses the future and may not be a sensible thing to do.

In any case I don't believe it would have been a sensible thing to do for the NCS. It ended up instead as a federation of communications systems, participated in by the State Department, the Department of Defense, the General Services Administration, the Energy Department now too — and it operates well today without the bureaucratic threat of a single system that you don't control. The Defense Communications System is 80 percent of the National Communications system; it has the dominant role. The director of the Defense Communications Agency is the manager of the National Communications Sys-

tem, and he manages by consultation. He consults, he persuades, he tries to achieve consensus — but he can't dictate, except under certain circumstances. He can dictate in time of war when certain executive orders have been issued; then he becomes a dictator. But up to that time he is a persuader.

It's a difficult way to try to manage something. It's surprising that it works, but it seems to. Every week, somewhere in this country, the President declares an emergency. Whether it's a flood, an earthquake, a tornado, a hurricane, the National Communications System staff, which is in the DCA Building, is charged with providing or arranging for communications support as needed by the General Services Administration's Emergency Action Group. When the President declares an emergency, certain loans become available, and certain communications assets can be provided for military or other resources. So every week in the year, on the average, there's a national emergency somewhere where military equipment may be on loan to a civil agency, or civil agency equipment is on loan to the local National Guard or to an active military unit, and is on the scene. And circuits are extended from the nearest NCS operating agency, whether from a defense installation nearby or from the nearest GSA office. Those weekly disasters exercise the NCS continually and it works quite well. Fortunately we have not had any enormous disaster, like nuclear war, which would further test it. And international communications have improved so dramatically that generally it's not been necessary to use NCS resources other than those of the DCS for that purpose. But it works, every week. Quietly, and without any particular noise.

What are the management problems, then? I've talked about management difficulty, with respect to closed-loop systems or unbounded systems, and single-user systems and multiple-user systems. What are the management problems you confront, particularly with the large kinds of systems you deal with today as Presidents try to orchestrate national power either in world affairs or in the smallest local kind of disaster?

Well, first, multiple users' needs often conflict, violently at times. Take the military case, with which I am, of course, so much more familiar. The Army fights from the field, the Air Force fights from its bases and the Navy fights from its ships. So to the Air Force air bases, and the communications connecting them, are very important. The Army is much more concerned with its communication when it deploys into the field. It doesn't care so much about the survivability of its camps, posts and stations. The Navy, of course, fights at sea. They all fight at different speeds and with different degrees of navigational accuracy. The result is that when you try to build a triservice system for the Army, Navy and Air Force, you've got three different speeds to contend with, three different geographical environments, three different doctrines and, indeed, three different languages. So multi-user systems are very difficult.

One other thing about multi-user systems like the Worldwide Military Command and Control System and the Defense Communication System is that since they are joint, the first question that emerges is, who is the sponsor for budgetary purposes? Now the Army, Navy and Air Force, generally speaking, want to buy, respectively, tanks, ships and airplanes. They aren't all that enthused about spending a lot of money on the Defense Communication System or the Worldwide Military Command and Control System. DCS and WWMCCS must compete in the service budgets with the hardware that the services are obligated to provide under the terms of the National Security Act. So first you must find the sponsor for a thing like the Defense Communication System or the National Commu-

nication System. That's sometimes hard to do. If you go to the JCS to sponsor it — the JCS, as you know, is a committee of the three military services — and if the Air Force's budget is being hit for a new satellite system that's going to cost half a billion dollars, which threatens the acquisition of a number of F-15 airplanes, then you know that becomes a tough budget decision within the Air Force. So the right sponsor is not always self-evident. The sponsor is the guy who puts it in the budget, who helps defend it before the Congress and who asserts its need over the services' other competing investment priorities.

After you reconcile all these conflicting user needs, and you have found a sponsor for whatever you want to do to the system, you then begin the planning, programming, budgeting and acquisition process, which is described in OMB A-109. The budget process breaks down the program into things called program elements, each a separate manageable piece. A program element may be a very low frequency communications system, or a high-frequency communication system, or some computers. And they're all parceled out among the program elements. They're assembled in the budget that way, they're defended in the budgeting process that way, and they carry that integrity all the way to the final budget submission. Moreover, OMB Circular 109 requires program management activity: development and fielding the piece of hardware to take place in somewhat similar, separately definable, manageable kinds of programs.

Those rules are built so that DoD spends most of its dollars on ships, tanks and airplanes; they don't fit command and control systems very well. Now you have the problem of justifying to the Congress a host of little programs: a VHF communications system, an HF communication system, a VLF communication system. And the Congressman sits there and says, "Why do you need three? Why won't one do? Why do you need computers here, why don't you use those computers over there?" So what you have to do is fit all these separate program elements under some sort of umbrella description — and the current title for that in Washington is architecture. So we have a WWMCCS architecture, a military communications satellite architecture, dozens of architectures; and they haven't really met the need yet, because we still think of them as separate little programs that you're acquiring — this particular kind of hardware for that particular use. Its relationship to the other pieces of hardware, and their particular use in the total context of C^3I, aren't readily apparent. Last year, in the 1980 budget, 63 separate program elements were submitted under something called the Telecommunications and Command Control Program. Half a billion dollars were cut from those 63 elements. One of the lessons Dr. Dinneen drew from that was they had not justified those 63 elements in terms of all the other elements.

It will be interesting to watch. Dr. Dinneen made a speech in December and one in January, and has had an interview in the January Armed Forces Journal. It appears to be a very serious, conscious effort on his part to justify all these separate little programs under one overall rubric, so that Congress can see the relationship of each one to the others. Very often if you eliminate one it affects the others in ways that are not readily obvious.

Oettinger. There are those who would argue that if you make it all visible it all becomes vulnerable as one unit, while if you put the items on different shelves some may survive even if a couple of them die, and you may be able to recover some of them later on. So that there's perpetual tension, it seems to me, between what you've described and alternative bureaucratic strategy.

Paschall. Exactly. But the reason I opt for the umbrella description is that over time all the separate elements that were hidden hither, thither and yon in the Defense budget have been all gathered together, through the assiduous efforts of all the auditors of the world, and it's all in the TCCP (Telecommunications Command and Control Program). So the days when we could play the shell game and hide the size of SAC Headquarters separately from the E-4 aircraft and the BMEWS radars — those days are gone. So you're forced into this.

Another thing has happened, started particularly by Congressman Mahon, who had an instinctive view that there were too many communications. The more we gathered together through the efforts of the Defense auditors, the more he became convinced that we had too damn many communications, and part of what you just said actually took place: it looked too big. How could you possibly spend $8 billion on C^3I? And that's the open part of the budget. (I myself don't know what others put under the "I" — it's hidden somewhere.) So it's a very large chunk and yes, if you expect to be able to justify it you've got to find somewhere to put it into a coherent whole. We have done a rather poor job of that on occasion in the past. I wish Jerry Dinneen much luck in his effort, because it's going to be tough.

Oettinger. A book by Harvey Sapolsky, "Polaris Missile Development: Creating the Invulnerable Deterrent," published in the late 1960s or early 70s, is a fascinating account of an altogether different style from what Lee is describing — which I suppose today's managers would regard as characteristic of the heroic days of open-cockpit flying, with the silk scarves and so on. The story was so peculiar in its creative subversion of the literal process that it would have lain submerged for some time had not Bob Frosch, now the administrator of NASA, become Assistant Secretary of the Navy and opened the archives to Sapolsky to tell the story. I commend it to any of you who are doing papers on or are otherwise interested in management, by way of contrast between what Lee is describing and what was and perhaps still is taking place in areas that were under wraps not for national security reasons, but for bureaucratic reasons, for its whole lifetime. One can only hope that similar things are going on elsewhere; but no one is talking about it.

Paschall. I don't know if it is being done. I, like you, hope it is. You look at how much or little publicity the SR-71, the strategic reconnaissance aircraft got, and how successfully it was done. I was attending the Air war college when President Johnson announced that. My colleagues were the select group of senior colonels in the Air Force, yet I didn't find one who knew anything about the SR-71; in fact, there were some who were downright insulted that they didn't know. So things like that do happen in the intelligence and the intelligence space programs. But I'm describing the open style, the "white programs" which, if any of you go to Washington, are what you'll be living with.

Student. Why do you have to give up the obscurity that comes with integrating the Congressional look at these programs? Why can't you treat them, for instance, as congressional oversight on the intelligence budget — maybe not all of it, but some good portion of it, leaving enough gaps in the picture so that outsiders don't know?

Paschall. When it's done outside the wraps of security, you are an open target. The Freedom of Information law, the requirements of the Armed Services Procurement Regulation

to debrief every unsuccessful contractor, the General Accounting Office, the Defense Audit Agency, the Congressional investigators — everybody looks at it.

Student. When you say "outside security," do you mean because it's not a classified program?

Paschall. Outside of compartmented security, I meant. So it can be top secret, and the GAO, and the Senate investigating staff, can and do look at it, but Freedom of Information doesn't apply in that case. When you get into compartmented programs, where access to the program is very severely limited, then you tend to be able to do things — the budget's classified, it's not seen openly; if you have a problem you throw money at it, and money will solve a lot of problems. You shortcut competitive processes. You don't have to spend three weeks writing a letter to the Comptroller General explaining why corporation X didn't win and why you really meant it when you put in your specification that this thing had to go 3,000 miles an hour, not 2,544. It's all those kinds of things.

If you have a scheduled slippage today in an open program — and by open I mean anything up to secret (that's relatively open in our society today) — you have to submit a report to Congress called the Selected Acquisition Report. The SAR goes over to Congress every time you slip so many months and every time you overrun so many dollars. That invites a lot of scrutiny. So managers tend to protect themselves. The most successful program manager I've seen in recent years is a close friend of mine. He was a very successful man — since he's a friend of mine I can say this, and I won't identify him — beyond his intelligence or, really, his capabilities. The reason was that he had a thing called management reserve, and when he went in with his budget for a particular program, he fought for management reserve. He estimated his program fairly carefully, he cranked in inflation and all those things, and then he said: "This is a highly technical, highly complex program, I need a large management reserve," and he fought for that. The management reserve was simply to pay for the cost overruns and schedule slippages he knew were coming. So he devoted his sales effort (incidentally, they don't teach salesmanship in the war colleges and they should, to further an officer's career if for no other reason) to selling management reserve. His Selected Acquisition Report went to the Secretary of Defense and to the Congress on schedule, within program. He'd consumed enormous management reserve but it was within program, so he got promoted. That's the kind of games people have to play to defeat the system, survive within it, or succeed within it. And I don't mean that in a derogatory sense. It's practical advice. If you do not include things like management reserve, if you do not take into account the real hard facts of life in budgeting and selling systems, then you should never believe anybody's estimate about what it's going to cost you in time or dollars. I finally came up with another of my laws, which says multiply everything by pi. Somebody once asked me, why pi? I said, well, three doesn't sound very sexy and anybody can multiply by two; but pi makes people stop and think "He must know something we don't."

I say that facetiously, but this system forces you to protect yourself in things like estimating — not deliberately overestimating, but you have to provide the cushion, because none of these systems will come in on time and none of them will come in on program in terms of cost. There are just too many uncertainties in the large technological systems we're building. There are uncertainties in requirements. The Army has decided it's not going to march at two and a half miles an hour, it's going to get in light vehicles and run

at 35 miles an hour, and that changes a requirement. And that has an immediate impact on any C^3 system you may be acquiring. So requirements change. The technology we're dealing with has revolutionized. The growth is astonishing, and so are the changes that happen. You get halfway down to a solution and somebody has a new invention that's the best thing since nickel beer, except that it's going to cost you four dollars to start over.

Student. From what you're describing it seems you'd be very tempted in this process to overbill the things you need just to get what you feel is essential. But you really have to do a lot of analysis on the margin, and in extreme cases you have to provide resources for justifying extreme solutions which you know you aren't going to get. How much of the resources do you devote to analyzing your requirements, things you really want? Aren't a lot of resources wasted in analyzing arguments for argument's sake?

Paschall. Let me answer the question in two ways. First, it depends on where you are. I note that you have two papers to do. One represents you as the worker and the other you as the decision maker. If you're the worker you're going to start out pretty much as you described. You're going to try to satisfy all of the operational requirements given you in the best way possible, and you're going to make your budgetary estimate do that comfortably and set aside a sufficient management reserve. That's what you start with. And then the system goes to work to scrub that down. The system starts with an assumption that your requirements are gold-plated, that they don't have equal importance; and as they bounce budget item against budget item your system will get skinnied down to some point. So the PPBS system, the whole approval process, will certainly get the gold plate out. At some point the anguished screams of the proponents of the system, you know, do penetrate the decision maker's hearing. (Up to a certain point those anguished screams are sort of pro forma.) But the system tends to scrub these things down. If you ask for a gold-plated system, one of two things happens. I could cite you one where the requirements were so gold-plated that it killed the whole program, and it was a tragedy. So there's a lesson to be learned there. You can't go all out — it endangers the entire program. But there are optional, nice-to-have features, and the whole process is designed to scrub out nice-to-have features. So, yes, I'm sure some money is wasted, I'm sure some things are done that ought not to be done. I'm equally sure some things are not done that should be done. But a large bureaucracy dealing with this kind of technology works surprisingly well. There is reasonable balance, I think, in most things we do. I don't know how to put that in anybody's MBA text; it's just the way the real world seems to operate, or at least my perspective of how it seems to operate.

Student. Do you think the budgetary process is adequate in judging a system and illuminating the peripheral, the gold-plated? Or will it tend to eliminate some of the wrong things and leave in some of the gold plate?

Paschall. Can I defer answering that until I come to how Congress handles this, and how to win and lose? Because you win some and you lose some. But through the whole process (and it's not just a budgetary process, it's also a technical approval process — when you read A-109 you'll see something at the beginning called MENS, a Minimal Essential Needs Statement), right through program definition, every step of the approval process and every examination that takes place (and there are a number of them), alternative solutions emerge to each of these kinds of problems. Each such alternative will have

its proponents, both in and outside government. They may be technical proponents; they may be vested interest proponents.

Now the tough part of the decision maker's job, particularly if he is not a technocrat, is that in these high-technology C^3 systems the differences between alternatives may appear very trivial indeed, and to the non-technocrat decision maker they sound way below his level of decision making, they're concealed with jargon, acronyms and those kinds of things, and they're often heavily larded with nuances of differing operational requirements — 3 mph instead of 2 mph, 2,554 knots instead of 3,000 knots. Yet there are people willing to die for that operational requirement. So decision making, confronting all of these alternatives, is very difficult indeed, particularly in the technical areas where you're chasing electrons through some kind of system. Senior decision makers, non-technocrats, get very irritated with the technocrat who's in there with his jargon, pleading for a particular form of spread-spectrum modulation as being absolutely imperative; and how much more does it cost? A couple of hundred million — spread-spectrum modulation for a couple of hundred million is meaningless to many people. So it's those kinds of things the whole process is designed to scrub — both the requirement and the solutions all the way through. But all that finally comes to roost in Congress, and I'm going to come to Congress soon. They have the toughest job of all.

One more of the management problems we're talking about. Would you believe that the reason the Worldwide Military Command and Control system is getting such bad publicity because "the computers do not work" is a disgruntled employee who once worked for me in DCA? A very articulate, persuasive man, an extraordinarily difficult subordinate who could not get along with his supervisors, whom we finally disciplined and, despite the difficulties of doing so in the Civil Service structure of those days, fired. Since that time he has waged unceasing war on WWMCCS computers. I have been to Congress several times, and I have talked with Jack Anderson's reporters (not voluntarily, but on the receiving end) at different times because of that one disgruntled employee who did not understand our real objective in a particular part of the program. So personnel management, particularly of key people, and during the approval process, when these alternatives are being worked, is something to be very careful about.

I keep coming back to people. As I think you know, technocrats are not noted for paying much attention to people; we tend to think of electrons instead. But people can get you in enormous difficulties, and any staff officer or decision maker who fails to take that into account is in for some trouble. Some of these are very pragmatic, practical kinds of things — but nevertheless the unhappy employee who is not articulate and not smart is no problem; what you have to do is be sure you have found the articulate one and satisfied him.

All this finally comes to Congress in the form of an appropriation, an enormous volume full of thousands of pages, and Congress has to decide how much of it to appropriate. Congress gets a bad press on some of this; they're accused of micro-management. During one of my losses, which I'll tell you about, I said they had auditors and investigators doing engineering. Also, the individual Congressman tends to listen to the contractor's alternative most carefully when that contractor is in his district. Moreover, there are power bases to protect within the Congress. There is no way to get a computer if Congressman Brooks from Texas doesn't want you to have a computer; he is the power base and even the leadership will not challenge him on that issue.

Congress deals with technical complexity increasingly using all those techniques. Congressmen protect their power bases because those power bases have some foundation. There was something fundamentally wrong with computer acquisition when Congressman Brooks got into it. In my view what was wrong has long passed by, but the power base remains to this day. The auditors do have a function; the investigators do have a function. But I would submit that their function is during and after the decision making, not at the front end of the decision making. On one of the programs I still feel badly about having lost, we had auditors who were making recommendations on a highly complex technical issue. They made their recommendation based on what they understand best: that which cost the least. The micro-management business — some of those Congressmen are remarkably well-informed about some programs; they will tell you, "Young man, I have been here 20 years and I've heard everything that anybody has ever had to say about that, while you've been coming to talk to me about it for two years. Now I know ten times as much about that as you do" — and in some cases they're quite right. They've been told everything, they've listened to every rationale, excuse, reason, justification, and so forth. So they do, on some issues, get very, very penetrating, both in their questions and in their attitudes.

So the Congressmen all have these techniques, and they're all used and, as I say, I'm not faulting Congress for micro-management. We send programs over there that are structured in such a way that it's a deliberate invitation to micro-manage it. I don't know how much of that is at their request, and how much of that is at our initiation — I suspect it's a combination of both. The Congressmen themselves are enormously busy. They have all sorts of pressures on them, of every sort in the world, and it's obvious that they cannot look carefully at everything. The last year I was at DCA I think we answered 200-odd questions about the DCA budget, which wasn't the whole Department of Defense Communications budget by any means — it was $70 or $80 million, something like that. We answered 40 questions about one $3.5 million item. Looking at a budget of $130 billion, with 20 questions on $3 million, is the kind of thing that gives people an impression of micro-management.

Where do all the questions come from? Another of the power bases in Congress is the congressional staffers. Never underestimate their power. It's delegated to them by the congressman or by the committee chairman. They are of uniformly high intelligence, in my experience. They may or may not be experienced in the particular field you're involved in. Mr. Snodgrass, who has often been criticized, came from the Agriculture Committee and overnight was assigned responsibility for the C^3 program in the House Armed Services Appropriations Subcommittee. He had an awful lot to learn about communications and about command and control, and he worked very, very hard at it indeed. Now the military people, those that I know, and those that I dealt with, very much respect committee staffers when those staffers are straight-arrow with you. I've known some committee staffers who could sit there and cut an appropriation or a program dramatically and you'd walk away feeling, well, he had to do it because that's what the congressman wanted and that's what the committee wanted — and you can respect a man who is doing what the elected representative tells him his job is to do, as long as he does it in a straight-arrow way. Now there are others, fortunately few in my experience, whom you cannot believe, and that's very difficult to deal with. One will tell you, "I'm going to support this," and then, as you walk out of the office, he cuts it in half. There are not many of them; in fact they generally get caught very fast in the system. Those I've seen like that

have been excessively ambitious, and want to make a big splash with their congressman, but it catches up with them. They are knowledgeable generally, they work awfully hard — I wouldn't trade jobs with any of them. They have been directed into this business of asking innumerable questions. The Congressional Record fills up each year with hundreds and hundreds of questions that appear as though they've been asked in testimony, while in reality they were sent over in a letter and we responded in narrative. I don't know what in the system has caused that, I don't know who reads that, other than the Soviet Embassy or the U.S. military who's trying to find out what we did wrong when we answered that question that got us that cut. One thing I think you can be sure of (reassuringly so as citizens): the Department of Defense's budget gets one hell of a scrubbing. Sometimes I think it gets too much scrubbing, and sometimes I think you have people who do not have technical knowledge (and here are my biases as a technocrat coming through), who get into areas of technical depth beyond their expertise. But that's how the system works. So if you want to be a power, you can try the congressional staffer route. But it's not an easy life. I assure you they work very hard.

Well, let's talk for a few minutes about how to win and lose.

Part of the Defense Communications System is the AUTODIN, a worldwide automatic data network. It was first installed back in the early 1960s as a part of the Air Force Communications Logistics Net. It evolved, and when the Defense Communications Agency was formed it became the Worldwide Joint Service Data Network. It was a pioneering effort, very successful, still used, very cost-effective, but it did not handle computer traffic very well, so it was decided that we would upgrade it to AUTODIN II, the second generation. Now, we had before us the example of the General Services Administration's Fednet, also a computer-based data communications system, which was intended to communicate data among the civil government departments and their computers. At the time privacy was a big political issue, and Fednet was killed (and doesn't exist yet) on the basis of a possible invasion of privacy. The same political fear has kept the FBI from putting together a computer communications network between itself and the state computer banks and data banks dealing with criminals. Privacy killed both of them.

So, at least, we knew enough to say "AUTODIN II is going to be secure, and we will engineer it in such a way that no one can get into anybody else's data bank unless he has been authorized to do so by the owner of that data bank." It was a hard time to get a new program in the budget in those days, and that's the first case we had to make. Then we sat down and listed all the current buzzwords in Washington and invented a couple more. We actually built a business plan for a military communications system. We showed how we were going to sell the services to the Army, Navy and Air Force and to the Defense Supply Agency; we looked at what the competition was — common carriers, Western Union, all the other things — we looked at several system alternatives, priced them all out and actually built a sales plan and a business plan and saw we were going to lose money for the first three years, but thereafter we were going to save money. At the same time we proposed to largely disestablish the old network (coping with one criticism Congress makes: that we keep adding things and never take anything away).

And we did one more very fundamental thing — which you have to do in today's open society — we made allowance from the beginning for a protest to the Comptroller General. We were competing this one, and in view of the changing communication structure

in this country right now, specialized carriers and others, we said, "We'll let anybody bid. We'll let them bid a government-owned system, a leased system, you can team, and it's not barred to anybody." And it was like comparing apples and oranges. Any time you build an evaluation process, where you're trying to evaluate competitively dissimilar things, building the evaluation criteria is a very difficult thing. We felt there was almost no way for us to do this successfully, so we documented everything right from the beginning so that when the protest was made to the Comptroller General we'd have our case file ready. We told the contractors, the bidders: "We're documenting every word of this, we're planning for a protest to the Comptroller General, and we expect that will happen." And we didn't get one. AT&T, the big bidder, was disallowed on technical insufficiency and there was no protest. So it did go successfully in that regard. It was rather a sales effort, and it seemed to work very well indeed.

Now, how to lose. My example is a second-generation secure voice network, AUTOSEVOCOM, Automatic Secure Voice Communications, enormously complex from a technical standpoint. A great many subjective judgments are involved in the different voice processing techniques used to achieve voice security. For example, we have, you know, a completely integrated military establishment, and I argued that a certain alternative voice technique did not reproduce a woman's voice nearly as well as a man's. It didn't work. Once again, the dollars drove it, but it was very complex and a very subjective matter to some people with 20/20 ears — but since I don't have 20/20 ears, one technique sounded better than another. Moreover, we sole-sourced this one to AT&T for a number of military operational reasons — not cost or even technical reasons — dealing with survivability and things like that. We did not have the full support of the community. The National Security Agency, which develops cryptographic devices, was divided within itself. That division soon became known to the congressional investigators and the General Accounting Office people who were put on it.

We just did this one all wrong, we really did, but we didn't realize we were doing it wrong. AUTODIN II looked like a management system, a communication system to do management improvements. It was servicing all those computers that are doing hiring, firing and retiring out of San Antonio and paying out of Denver, so we approached the secure voice network as though it were a military operational requirement, and we mounted up all the four-star generals we could gather together and got them to say how important this was as a military operational requirement, and we gathered together the engineers and said, is this the only way you can do it? — and we fell flat on our faces.

The point is that there was a time when you could go to Congress, particularly in the days when the old established committee chairman could pretty well drive the process, and convince that one individual, that committee chairman, that a program thing was valid as a military requirement, tell him: "My military advice to you is, don't ask all those questions, just vote it." Well, that's no longer possible in Washington. You have got to demonstrate it, you've got to prove it, and just saying you have a bonafide military operational need just won't wash any more. There was a time in the FBI's existence when Congress wouldn't have challenged anything they said we needed in the way of a communications network. But there are very few things now in Washington that won't get a challenge. An agency head who goes to Congress and says, "This is absolutely vital and essential to my needs" — if he can't prove it, if he hasn't done the advocacy business, or the sales job, or his preliminary work properly, he probably isn't going to get very far.

The final win — and it was a narrow win, almost a classic case of how to bring industry pressure to bear on a selected element of Congress — was the next-generation defense communication satellite. One company is building the current satellites. We'd let another contract to another company to develop newer, better, more modern satellites. The issue developed around whether you ought to settle for a minor upgrade for less money, and continue to buy the existing satellites. That proposal was sponsored, as you can guess, by the guy who was making the existing satellites. The issue came down to a call from a senator from the state in which the new contractor was located. He wanted a letter that related the importance of that new satellite to things like the Liberty and Pueblo incidents of a few years ago, which is a little difficult to do; but I succeeded in doing that. The issue finally came to a Senate/House conference; the senator circulated a Dear Colleague letter with that statement of operational military requirement, and it narrowly won the day. Does that violate what I just said to you, that those kinds of statements are not any good any more? Well, they still are if you have an influential senator or an influential congressman who's willing to take that letter and become your advocate in Congress. So those are some of the ways you win and some of the ways you lose.

Finally, I'm going to list what I think are the major C^3I issues today. Anybody who can solve these eight problems, you see, can become a hero in many ways. The first is how to handle the business of telecommunications protection. The way we do it today is to put a cryptographic box on every line, or on one big radio system. Very expensive! You can afford that for military applications, where you have classified military information. But what about all those conversations dealing with unclassified elements and pieces which, however, when assembled even by a relatively inexperienced person can give you a coherent picture of what's happening? Is the size of the wheat surplus in the United States of interest? It would seem to have been when we were negotiating with the Soviets about what price they were going to pay for all that surplus. There's a large amount of information flowing through microwave systems and satellite systems in the country which is readily available to even an unsophisticated interceptor. In Vietnam we found the Viet Cong (not the North Vietnamese professional military but the Viet Cong, in what they call "spider holes" with Heathkit radios) were reading our communications. And the problem of protecting against intercept of privacy telecommunication pertains to much more than just classified military information. It extends to point-of-sale things, for example. As I buy an item and the sales clerk punches it in, if that also debits my bank account — in other words, if I pay the bill at the same time I buy it through a fund transfer arrangement — privacy and protection of telecommunications is equally a problem there.

The second problem is survivability. There are really two ways you have to survive. Most people think of survivability as being one thing: you are shot or not shot. Physical survivability is important, and most survivability conversation, thinking and studies deal with physical survivability. But perhaps an even more serious problem today, given all the electronic systems we use, is electronic survivability — being able to resist an electronic attack. In the 1967 Yom Kippur War the jamming the Egyptians mounted against the Israeli communications was so severe that the Army had to lay wire out in the desert, and the Air Force, at its bases in Tel Aviv, was forced to use runners to get messages from the control tower to the aircraft. They could not launch aircraft from the control tower. The Israelis literally lost command and control for about thirty-six hours under Egyptian jamming attack. Yet the Egyptians were using, not really hand-me-downs, but certainly second-level electronics jamming equipment.

The Soviets are very candid. Their open literature on military doctrine (not classified stuff) says they intend to physically attack one-third of the enemy's command and control — bombs, weapons, sabotage. They intend to electronically attack — that is, jam — another third of it. With the remaining third they do not feel he will be able to effectively manage his force, and they expect to have a decisive advantage in combat.

So the defense against jamming is a major problem as well as how you survive an attack and, having been damaged, reconstitute what you had in communications, command, and control. Now some of these problems can be solved rather easily by throwing very large amounts of money at them. But that's not a very sophisticated solution, and it's not doable in many ways today. Other problems require engineering advances; some may require some inventions, and a lot of them will be around for a long time.

The third problem is difficult to describe; it's what is identified as the intelligence operations fusion problem. There's a lot of intelligence information, and it's gathered from various sources. One of the basic tenets of intelligence collection is that you must protect your sources, otherwise you'll lose them. Very few people must know about the source. So intelligence over the years has grown up in compartmented ways. That mindset says "We need to protect everything about intelligence," and if you're not a member of the community and you don't have all the compartmented clearances, it's hard to get it all together. But some intelligence collection is in near-real time, and it's getting precise enough so that it can be given to a battlefield commander and he can make use of it. So what you want to be able to do is be sure that somehow the intelligence useful to the operator, the commander and the staff officers gets disseminated to them — not in a weekly or daily intelligence broadcast or message whose source has been sanitized, but directly from the source — and still somehow protect where it came from. It's an engineering problem, I think, and an attitudinal problem more than anything else.

Software is the next one. First, how do you achieve multilevel security so that your software, your data base, can't be spoofed or changed without your knowledge, or extracted from to get information? It's often called the multilevel security problem. The solutions are hard to implement, and they have an effect on throughput — that is, how efficient your system is. The aspect, though, that's not often talked about is verification: how do you know the computer program's going to work as you want it to when it meets an unexpected situation? There's a classic case. The French had a meteorological satellite up several years ago, and they put into the telemetry a command generated by a computer to reconfigure something, or reposition the satellite, or point the satellite at something else — I don't recall the exact details, but I do know what the result was. A glitch in the software turned the satellite off. This was shortly after it had been launched, and it was a dead loss; they never could get it turned back on again. Now how do you verify command and control systems and management systems, especially as you get more and more into near-real-time situations and people are interacting with the computer? How do you verify software so it won't do something unexpected to you at the worst possible time?

The fifth problem is the cost-benefit equation. We've talked about the value of command and control and management systems in improved management — saving money, using systems analysis techniques to make investment choices. It's very hard to quantify the benefit you get by spending a million dollars on a command, control, and communication system. In terms of numbers of dollars saved in buying F-15s, people have subjective views about what it's worth. So anyone who sits down to justify what the trade calls a

"soft-kill capability" — well, computers don't kill very much, compared to a "hard-kill capability" like an F-15 or an A-10 or a tank. The systems analyst can do marvels with the tank — probability of kill, first sighting; add a laser or a laser designator to it and the probability of kill goes up to a measurable degree. It's harder, though, to quantify the benefits if you add another radar which gives you a second way to identify a Soviet missile and decide that it is indeed aimed at you. People who deal with C^3I systems analysis and cost-benefits studies would be much happier if they had some way to do that.

I alluded earlier to the sixth problem, the changing domestic communications structure, as being a fact of today's U.S. environment. Ninety percent of the Defense Communications System in the United States is leased; we have very few government-owned communications systems. Ma Bell has provided the bulk of that over the years. They have put transcontinental cables four feet underground in sand and built 50 to 100 pounds-per-square-inch manholes and underground facilities, and they've done all this without charging Defense separately for it. They've routed microwave systems around rather than through cities. They've done many things that are in the defense interest and they say that is because one of the first purposes of the Communications Act of 1934 is to provide for the national security and national defense.

Now there are a lot of new competitors on the street — the MCIs, the Southern Pacifics — and we're going into a competitive, intercity world from a communications standpoint. Most of the new competitors have tried to minimize their investment; they want to charge the least amount possible because they have to compete with something that already exists and is very large indeed, the Bell system. So they're not going to build the additional features of redundancy, restoration, and hardness that we like in military systems. But the Armed Services procurement rules say very simply: you will compete.

So the military people who are acquiring communications, largely leased in the United States, over the next few years have got to learn how to live in a different kind of world entirely. If the catastrophe occurs and we have all these separated communications systems, how can they be interconnected to restore, reconstitute and revive the nation after a nuclear attack? There's no apparent way to do that today, though the Department of Defense's position to the Congress, at least as reflected in the Van Deerlin bill, would provide for something like that (it's not clear how all that's going to end up).

Then there is the seventh problem: information needs, or information overdose; we mentioned it earlier. It's very hard to define. The typical staff officer, when asked what he wants in the data base often responds: "Everything, because I don't know what the Chairman of the Joint Chiefs of Staff is going to ask me next." I can cite you one instance from the Israeli-Egyptian War, or perhaps it was the Cyprus crisis. The White House asked about the possibility of putting some troops at a certain place in a hurry. There was a Marine landing craft in the Mediterranean on an exercise schedule. The Marines were scheduled to go over the side on landing, into the landing boats and then ashore, to practice an amphibious landing. The first question that occurred to the staff officer was, have the Marines gone over the side of the landing craft yet? And, you know, who knows? Well, what good is that computer? Things like that, said in a moment of tension, leave impressions on people; so the net result is that, when somebody asks what you want in your computer, the almost inevitable answer is "everything" — and real time. That obviously will not work.

So defining what you want and deciding on timeliness, and when to update, and all those kinds of things is very difficult indeed — and if you're not careful how you do it, you end up with much more than you need. Then the decision maker gets a bad case of indigestion called information overdose. When that happens to him he's confronted with so much information that he can't figure out which is important to decide. I think we saw some of that on the part of the Nuclear Regulatory Commission when they were trying to decide what to do about Three Mile Island, and ended up deciding the best thing to do was prepare a press release, which is focusing entirely on the wrong problem. That can happen to you.

So command and control systems and management systems both have the same kinds of characteristics. You have to find some way to control that information, or display it in such a way that the important elements emerge, so that what is important is driven to the attention of the decision maker.

And that brings us to the last problem, which is almost a national strategic problem: decision time. Our structure, our strategy, our military forces are trained and will obey the order that says only the President can release nuclear weapons. Seventeen minutes is the time of flight from the normal Soviet submarine ballistic launched missile patrol distance off the Atlantic Coast to the White House. So from the time somebody sees something launching on one of those satellite sensors, or one of the radar sensors along the shore, seventeen minutes is decision time. That's a very short time indeed. Moreover, people don't want to believe news like: they have launched, the world is coming to an end, it's time for you to launch in return. President after President has called for options, more options. Each option called for imposes an enormous demand and strain on the command and control system. So how are we to solve decision time problems? How can we make warning completely credible to the President or to his successors? How do we ensure that the successors can communicate, can establish contact with the force commanders to execute the retaliation or the strategic reserve, or continue to negotiate, or whatever? There's a very difficult task. Technocrats talk about computer-based executive aids, about making warning more and more credible, and they tend to forget there's a man who's got the world's fate in his hands, and he's got seventeen minutes, and that's just not very long. That's why military doctrine is so emphatic about building a force structure that will deter war. Deterrence is simply a state of mind, and a command and control structure capable of absorbing a strike and functioning thereafter, or being reconstituted to execute the strategic reserve, is a very important part of that deterrence state of mind. The enemy must believe he could never decapitate us, in the sense of killing the decision maker and preventing the decision to launch from being transmitted. That's why command and control systems are so important to the military, and that's why we've learned so many lessons over time.

Student. Are these worst-case probabilities a significant factor in the seventeen minutes? Are there situations in which a significant fraction of that seventeen minutes will be used up just getting the first message to the President?

Paschall. No, one or two minutes is consumed in getting the first message through. In one or two minutes the President knows there's something radically wrong. That leaves him about fifteen — that isn't a very comfortable number to live with either.

So that's why to me, with my military bias, the difference between a command and control system and a management system is just the fact that the kind of top-level command and control systems that control this nation's military power do have decision times that are near-real time. Management systems you can be much more comfortable with.

Student. Can you enlarge on the situation about two months ago, when the system for about six minutes appeared to indicate that an attack had been launched?

Paschall: Yes. At one point in the system a computer test program got on the communication line inadvertently, and passed what was known as a missile warning message to some locations. The system is arranged so that things have to be voted on and go separate ways — all this has to be done very fast. But the way the system was designed, it was known within something like thirty seconds that it was a false alarm, because it didn't work through the voting process. It was a computer software glitch compounded by a personnel error — people, procedures, time and again will cause you difficulty. But it caused no particular alarm within the military community because the negative vote was almost instantaneous. And it was a valid negative vote.

Student. The American system is a loose connection of various communications and sensor systems. Do the Soviets have a more unified (how do they interpret that word that you were talking about earlier?) command and control structure?

Paschall. First, the WWMCCS is more tightly coupled than the national communications system, which is very loosely coupled. To answer your question, yes, our system is much less tightly coupled than the Soviet system, reflecting two different styles of government. The Soviet system is hierarchically very rigid, very tightly coupled, but it takes into account the fact that destruction can and will occur. The Soviets make heavy use of something called skip echelon — that is, Moscow can talk to the military district, or it can talk to the missile battery, or whatever. They've spent much more money than we have on hardened command centers; they have them by the thousands, literally. Very little of their capability will sustain a direct nuclear hit, but enough centers will survive collateral damage to give them a very survivable command and control posture. Compared to the Soviets' rather rigidly, hierarchially structured operations, our people exhibit more initiative. In the absence of direction from higher headquarters they tend to do what they think is best, and it's often better than what our headquarters think they ought to do, too, because they're on the scene. The flexibility and looser coupling of our system is an advantage, I believe, even given the fixes that the Soviets have taken on skip echelon and things like that.

Student. Does the Soviet hierarchy impact negatively on the problem of decapitation? Are they more susceptible to it?

Paschall. I don't believe we would ever strike first, but if we did, with no warning, their whole structure, their whole society, is much more subject to decapitation than ours. We have 50 governors who'd want to be President on the day after the attack here, and probably 75 senators, but in Russia the system just doesn't work that way.

Student. Do we know if they have a succession system similar to ours?

Paschall. I assume they do; it would be foolish to assume otherwise. I suspect there are a lot of rigidities in it.