INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

Strategic Connectivity
Richard H. Ellis

Guest Presentations, Spring 1982
Richard D. DeLauer; Hillman Dickinson; Gerard P. Dinneen; Richard H. Ellis; R. Thomas Marsh; Thomas H. McMullen; William G. Miller; Richard G. Stilwell

December 1982

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-82-3

Strategic Connectivity

General Richard H. Ellis
(USAF, Retired)
Formerly Commander-in-Chief,
Strategic Air Command

General Ellis has recently relinquished responsibility for the nation's major nuclear deterrent force, which includes bombers, tankers, reconnaissance aircraft and intercontinental ballistic missiles. He also wore a second hat as head of something that has a great deal of significance for command, control, communications and intelligence: the Joint Strategic Connectivity Staff. He began his career as an aviation cadet in World War II, rising to deputy chief of staff, Far East Air Forces before the war's end. He has been vice commander in chief of USAFE and has commanded the 6th Allied Tactical Air Force, Allied Air Forces in Southern Europe, the 16th Air Force in Spain, Allied Air Forces Central Europe, and finally USAFE itself. He directed the Joint Strategic Connectivity Staff at Offutt Air Force Base from its founding in summer 1980 until his retirement, and directed the Joint Strategic Target Planning Staff, also at Offutt. He brings this wealth of experience in operations, war plans and policymaking to bear on the C^3I problem.

Ellis. I want to emphasize the informality of this. What I'm going to talk about is mostly a collection of things that have happened during my career. We may tend to feel today, for instance, that C^3I, or strategic connectivity or whatever you choose to call it, is in deep trouble. It may be well, though, to think back a few years to some of the things that we had to make do with during the cold war days of the 1950s and 60s. In that light we may indeed be making progress. I'll try to define C^3I as I saw it in the JSCS, the Joint Strategic Connectivity Staff. That was one of my three hats. A second was SAC, and the other was the Joint Strategic Target Planning Staff (JSTPS), which was organized in 1960 as the last act of the Eisenhower administration and in effect established a staff at Omaha composed of people from all the services whose sole task was to draw up the nation's nuclear war plan.

I should point out, parenthetically, that in the 20 years of its existence the Strategic Target Planning Staff has developed into what I consider the finest military staff in the world today. The reason it's had such success is that it hasn't been loaded with a lot of other things, as the government usually does — they give you more and more things to do, and the result is that you don't do anything right. But that's not the case with this staff, numbering today some 325 or 350 people who draw up a plan of amazing complexity in scope and simplicity in execution. Of course that's the key to command and control. If you can't execute, and execute quickly, everthing else is for nought.

The JSCS was formally established in fall 1980, and I hope it doesn't take 20 years for that staff to reach the degree of competence that the JSTPS has achieved. I don't think it will, because of the support it is getting and the prestige it has already accumulated in Washington and among the nuclear commanders-in-chief.

Let me just define the CINCs I will be talking about. The nuclear CINCs are those commanders-in-chief who command nuclear strike forces and have a responsibility in the nuclear war plan; there are four of them:

my old hat, CINCSAC; CINCLANT, whose headquarters is in Norfolk; CINCPAC, in the Pacific; and CINCEUR, over in Europe. There is another CINC who plays an important role in overall strategic connectivity, Commander-in-Chief NORAD; he doesn't handle nuclear forces or nuclear responsibilities, but CINCNORAD is the man who tells the president, the national command authority, that we are indeed in trouble and that such-and-such is happening to us to the best of our ability to identify it.

The strategic connectivity staff is composed now of only about 30 people. CINCSAC is the director. It includes a Navy Admiral, Paul Tombs, who as many of you know is a very capable and successful nuclear submarine commander. He has rapidly become recognized as the person who, if you're fooling around in Washington and not getting on with the job, is going to be beating on your door, and he does it very well and very effectively.

Well, let me just say that strategic connectivity is only one aspect of C^3I. I call it strategic connectivity because we're not talking, for the most part, about how we fight theater nuclear war, how we control it or what is required. That's an entirely different problem — and it really is a problem area, because if you think we're in trouble in strategic connectivity, we're in terrible trouble in the battlefield theater area, and I think anyone who has any feel at all for it will know the problems and understand why.

Oettinger. Let me just interject — the reading in Cushman's work* makes that link clear.

Ellis. Well, strategic connectivity itself is highly centralized, in that everything that is done in that system has one purpose: to get information to the president, the national command authority. In execution, though, it is highly decentralized, because everyone all through that net, all the way from the president down to the lieutenant who sits out at the radar site in Thule looking down the Soviet Union's throat with his radar, has fixed responsibilities. There are certain things each individual is required to do, all of which must be accomplished if the information is to get up to the authority who has to make the final decision which, in turn, must get to those whose job is putting the decision into action.

Now, historically there's really nothing new in military C^3I. It's only the term that is recent. The activities that make up C^3I have been around since the beginning of warfare, and their purpose has always been the same: to get intelligence on enemy movements to the man who has to meet them, and to get his instruction sent back down. You will hear some people claim we only need a one-way system: forget it. It's always been two ways. And when people say, ''We'll have a one-way transponder sitting on a satellite, that'll serve the purpose,'' well, it won't serve the purpose. As I get into the definition of connectivity, you'll see that there's more to it than just execution or just decision making.

Let me first talk a little about C^3 as I've seen it over the years. I'd like to go all the way back to World War II. I was a combat pilot and I was on the receiving end of orders. I was in the mission execution business, but at the same time my comrades and I were a very key part of the decision-making process, because we were the ones who reported what we did. And that is one of the first uncertainties that enters into the whole C^3I problem: what did you do and what else has to be done?

I can speak from first-hand experience. We were engaged in low-level attack. We were right down on the targets, bombing and strafing them at treetop level. There were certain things we saw and reported, and yet it turned out, when we got the photographs back, that we were wrong. And if you think that's changed today, you're wrong, because it hasn't. What is reported about the battlefield or the airspace, and the actual fact of the case, may be two entirely different things. And that's why this is an iffy business, and it's why, when people talk about firing on warning, or launching on warning, they're in a very risky area. It's dangerous, in my opinion — very destabilizing.

The first time I was exposed to nuclear command and control was in 1952, when I went overseas to England with the first tactical nuclear weapons unit deployed to Europe. It was a very highly trained force: two wings — 75 fighters, and 50 medium bombers. We had our weapons, we had our training, we knew how to deliver. We had state-of-the-art technology in delivery systems. We were ready — but we had no war plans. NATO didn't know what to do with the weapons when we got over there. It's surprising, but they had to reorganize part of SHAPE headquarters in order to pull the nuclear war plan together. Some of you who have read your history books may remember that SACEUR

*See John H. Cushman, ''C^3I and the Commander: Responsibility and Accountability,'' in *Seminar on Command, Control, Communication and Intelligence, Guest Presentations, Spring 1981*, Program on Information Resources Policy, Harvard University, Cambridge, MA, December 1981.

brought General Norstad up to SHAPE as his deputy. General Norstad was responsible for the first war plan, and he pulled some of us from the 49th Air Division over in England to come and help do it. We were the so-called experts. We wrote the first plan in 1954, and I can look at the European and the NATO plan today and still find some familiar words. We used to call it the Atomic Strike Plan; today they call it the Nuclear Strike Plan. That's a massive change! But other things really have changed.

It was a great time, the early days of the alliance. General Eisenhower had just left and John Gruenther had taken over, and one felt a sense of accomplishment that fourteen nations were in an unparalleled military alliance with clearly defined responsibilities aimed at one objective. The areas of responsibility are clearly defined, and of course today that's one of its problems. People try to make more out of the alliance than it was built for. It's not an economic organization. It's not an organization to worry about the problem of the South Atlantic or the Indian Ocean. Maybe it should be.

When I came back we went to Texas in 1956 and helped organize what amounted to the first rapid deployment force, except that we had another name for it: the Composite Air Strike Force. That's when we learned to refuel fighters inflight, one of the great steps forward in tactical aviation. We had always thought of tactical aviation as confined to the theater. But with inflight refueling, the fighters could fly across oceans without landing and could be thrown into the battle a lot quicker than they could ever have been before. That's what war is all about: get to the enemy as soon as possible, with as much surprise as possible.

We had our introduction to command and control there, when we tried to control that composite force from Texas for instance, when it was exercising in different places. It worked, and it was the beginning of what we call "projection of forces" to protect the areas of national interest of the United States. We've done it many times since the 1950s; we did it in Vietnam. We've done it with Korea. We've done it on several occasions when we have reinforced Europe. We did it down in Central America, in the Dominican Republic. So the rapid deployment force, which people say is a new idea, is not so new.

There was a great jump in military command and control at the battlefield level in the 1960s and early '70s in southeast Asia. The satellite came into use for the first time. People saw it then (and I guess some still do) as a mixed blessing, because it put Washington in immediate contact with the battlefield commander. Battlefield commanders normally aren't very interested in that. But it also allowed rapid dissemination of intelligence (such as it was) and information to the very highest levels more quickly than ever before.

We first used our command and control aircraft to good effect in those days when we had a combined strike. The Navy and the Air Force, with supporting tankers and electronic warfare aircraft, combined forces for raids against the Hanoi area. They were controlled in the air by command and control aircraft that were in constant touch with all elements of the strike force. And they were able, on the spot, to adjust for events not anticipated in the original strike plan. That was a great step forward. It has resulted in what we now call AWACS. People call AWACS a miracle system — but in fact it is a very simple system. It has a few computers. It has some excellent communications, and it is crewed with people who know what to do with the equipment and information obtained.

You might be amused by some of the exposure I had to NATO command and control. In 1971 I was sitting happily in Wiesbaden, Germany, as vice commander-in-chief of U. S. Forces Europe, and unexpectedly I was sent to Ismir, Turkey (known in the old days as Smyrna, Asia Minor), as commander of the Sixth Allied Tactical Air Force. That is the easternmost projection of NATO's air power. The forces available to me as commander were Greek and Turkish air forces, and I had a staff of mostly Greeks, Turks, and Americans, with a sprinkling of Italians and British. My communications — when I walked into my office, I'll never forget the terrible shock. The phone looked like a World War I instrument. I picked it up, finally somebody answered, and he sounded like he was on the other side of the world. And I said "Who is this?" and his voice said, "I'm your secretary." He was right outside the door.

Now, it wasn't really that bad. We had the ACE High net which stretched all the way through Europe, the Allied Command in Europe HF net, which we were able to encrypt. We had a US net that was in very good shape, a very important net called, I think, either the Graveyard or the Tombstone net. That was the net that came from Washington to US officers, usually in the rank of lieutenant colonel, who were in charge of the nuclear weapons that were earmarked for certain NATO nations that helped maintain NATO's nuclear alert. Those US officers were the people who had to get the word to the NATO people and release the weapons to NATO forces in the event of war. I used to wonder if we'd ever get the word in time to be useful.

There has been progress in the intervening years. We now have a NATO satellite system that, together with the US satellites, are in constant contact with all the NATO regions. I guess the one thing that was most interesting to me when I went back to NATO in 1975 as commander of US Air Forces, Europe, were our efforts in command and control. We had just built a large command center at a place called Boerfink in Germany — converted it from a German underground air defense shelter which was state-of-the-art in the early 1960s — a magnificent facility, some 50,000 square feet, I think, and protected against conventional bombardment. But the problem in Europe then, in the mid-1970s, and to a large extent today, is this. There are some very sophisticated commercial communications nets in Europe, the PTTs — all the countries have them, especially in western Europe. But they have difficulty talking to each other, and they could not talk to military systems. One of our challenges was to make arrangements and agreements with the various countries under which we would provide them compatible switching centers and terminals in exchange for permission to use certain frequencies on their nets in wartime.

That's a slow business. You're dealing not only with the nations themselves (a lot of those nets are nationally owned) but with commercial companies that are looking for profit. Our government, of course, added its usual bureaucratic complications. All in all it's very difficult to get the interface we wanted.

I think the best example is the German Grundnetz. It is an underground system, built by the German national communications system, with access channels into the net throughout Germany. With it one can reach all of the German military. But it couldn't talk to the American military, or to Belgium, or British forces. We made an arrangement with the Germans under which, in return for use of certain of their nets, frequencies and lines, we provided them certain encryption material. It'll work — but the point of this story is that there's a lot of technology over there, in being, and the problem is to tie it all together into a cohesive net that is available to the NATO military as well as to the national, commercial and governmental organizations.

Now let me get to strategic connectivity. There are many definitions, but the simplest is that strategic connectivity includes the hardware, the software and the people necessary to get information on nuclear attacks against the United States to the president so that he can get a timely execution order down to the units. That's the mission of our strategic network. Before I describe its different elements, let's look at what we did for so many years before, when it was a relatively simple system. During the 1950s and '60s there was only one mission: to get the word out, to execute. We weren't too concerned about what happened afterward. We had nuclear supremacy, and then superiority — but then gradually that started to fade in the late 1960s.

In the early 1970s the Nixon Administration decided that something had to be done. The President couldn't be left with just this one alternative of "Throw it all or nothing." Mr. Schlesinger's "flexible response" policy was ratified by an NSDM in 1974. You might say it was a long time coming. I can recall Mr. Schlesinger's coming in to the air staff when he was head of the strategic section of Rand in the middle sixties and talking flexible response, but it was the sort of subject that people weren't ready for; it was ahead of its time. Besides we still had sizable superiority; we believed all we had to do was let go and that was enough to deter the Soviet Union. In the mid-1970s, however, we realized that that day had passed, and our policy has gradually evolved since.

Today the latest presidential decisions are spelled out in Presidential Decision Memorandums 53, 58, and 59. Number 59 is actually the policy, while 53 and 58 state the command and control, and the continuity of government, that we must have in order to carry out the nuclear policy. These PDMs are, of course, subjects of some complexity and some debate, and have been since their promulgation in the spring, summer, and fall of 1980; but they are the drivers behind the big advance we have in strategic connectivity today. They set the policy and the priorities, and, given the right kind of organization to implement them and the resources in terms of money, will provide us with the strategic connectivity we hope to get eventually.

Now let's talk about the elements of strategic connectivity. I say there are seven elements. The first is the attack detection network. That includes the warning satellites, infrared, Sigint, Elint, the BMEWS, PAVE PAWS, and COBRA DANE radars, and other intelligence assets which would indicate that the Soviets are in the process of undertaking an attack against the United States. Some of those systems themselves are very old, like the BMEWS, though they have been upgraded from time to time. Some are very new and sophisticated, like our synchronous satellites. But there are things that we didn't think about when we built those that have come under serious discussion in recent months. I'm talking about the atmospheric explosion or detonation of nuclear weapons with resulting EMP, blackout and the scintillation that can "blind" these "sophisticated" satellites. That's being worked on. We know they have frailties. You've got to remember too that we don't know as much about any of those phenomena as we would like to know, because we stopped our atmospheric testing many years ago. The Soviets tested in the atmosphere longer than we did, and a lot more extensively than we did, and consequently most knowledgeable people believe the Soviets know more about the atmospheric and exoatmospheric effects of nuclear blasts than we do.

The second element of strategic connectivity, as we define it, is attack characterization: gathering all the intelligence from any possible source, using the most sophisticated and fastest means of collating it, and coming up with a decision on what it means. The information gathered by the detection elements has to be sent back to the place where this characterization is done: NORAD in Cheyenne Mountain. Now, just getting it back is a problem in itself. We use satellites, we use transatlantic cables, we use high frequency and very high frequency and low frequency to get the information there. But a lot of things were overlooked as we built those systems. For example, in 1978, when we did a study I'll talk about later, we found that one of the terminals from one of the overseas sites was in an AT&T building in San Francisco that was unprotected. Anyone could just walk in the door to a switching center with the name of the originating terminal on a sign. In other words, it identified the overseas station, and you knew right away that this was the United States terminal for that information, highly vulnerable to anything anybody wanted to do to it.

The NORAD commander's job of attack characterization is unique to him. Only one other individual or organization has that responsibility: the president.

Student. Does all the information from these detectors go in to NORAD as raw data, or is some of it processed?

Ellis. Some of it's processed at the site. They'll see something on the scope at the site, for instance, depending on what kind of site it is. The lieutenant there is trained to know what he's looking at; but what he sees at a terminal from one of the synchronous satellites and what another operator sees at a terminal from one of the radar sites may be two entirely different things. Some people in the command net may say, "I don't want to talk to NORAD, I want to talk to the site." But what you've got out there is some young fellow with a couple of years of training who is looking at a phenomenon he may never have seen before and making his judgment on what it is. Whether one wants to rely on that as an ultimate judgment is something else. You have to instill the discipline, the professionalism in those sites that you have in every other part of your nuclear system. We started putting controllers at the sites who had finished a tour as a missile commander in SAC — usually three years as a missile commander sitting in an underground control center. That gave us controllers with discipline and understanding of procedures we couldn't get any other way. But at that end it's an iffy business. All the information comes in to NORAD. It's ground up in their computer programs and presented to them in a manner of minutes, in some cases seconds, as fused information, which indicates to the commander out there that such-and-such is happening. All one can do is hope that the software isn't faulty, or the hardware isn't spooky, and the person is not making a hasty judgment. Things can go wrong.

Student. Do you have some kind of system of checks to guard against that?

Ellis. That's what the humans are in the line for. The human is in the line all the way up to the president. CINCNORAD doesn't release the nuclear weapons. All he's doing is saying, "This is what I think is happening to us." For example, at SAC direct readouts are provided from the sites, too. But that information isn't used for attack characterization; rather it is used for force survival. SAC may raise the level of alert. CINCSAC may even launch the force under positive control, depending on how urgent the threat is. But the one place that the attack characterization is supposed tc be made is NORAD, and that's why we have a four-star general there whose primary job is to make sure that he's going to do the right things when the time comes; and hopefully he will. That's the second step.

The third step is the decision by the NCA. He's going to have to take the final attack assessment and do all the other things he wants done as part of his decision-making process — political and other considerations that the average military man might not even be aware of. He's going to make a final decision, and his decision could be any one of thousands of choices. People talk about flexibility in the strike plan — there are thousands of alternatives in this plan, any one of which he could pick, but making your selection isn't as bad as it sounds. It is very organized, and people at the far end will know what to do if they get the message.

The most exciting part of this whole sequence to talk about is how this man makes a decision, and I want to forestall any questions on that right now. Let me just say that he's got the responsibility — he knows he's got the responsibility. It's established in law. Obviously a man with that responsibility is going to make provisions for contingencies when he may not be available, or is incapacitated. As SAC commander, I was always satisfied that that was taken care of, and I think that's where we ought to leave that subject. Everybody likes to know exactly who's next in line, and who does what, but that's the president's decision and he's not going to say much about it. I don't know of any president who's ever discussed the subject publicly.

So now there is a decision, and it must be disseminated. The decision goes to a staff that's in constant contact with the decision-making authority, the CINCS and the fighting forces. They format the message. Much of the formatting is already done. It's the staff's job to get the message out to the forces that are going to execute the plan, and this of course is time-critical because our seat of government is on the coast. This part of the process may have a life expectancy, in some scenarios, of somewhere between 11 and 13 minutes — the delivery time from the patrolling Soviet SLBM submarines. So these things have to happen fast, and they have to happen accurately. One tends to think about the big parts of the sequence like the decision, but the little parts, like getting out the execution order, are just as important, because if you don't get it disseminated properly and in a timely way, it isn't going to get executed. That's why there is not only an NMCC at the Pentagon in Washington, but a national emergency airborne command post (NEACP) which also has the capability to disseminate the decision. It is disseminated through every mode available: landlines, various kinds of radios, satellites, and some others that we probably shouldn't get into at this point.

The fifth step is execution of the decision. Again every communications system is simultaneously exercised by the people receiving the order — the commanders, whether they are SAC, LANT, PAC or Europe. For instance, SAC has a primary alerting system, an automated command and control system, AFSATCOM, the emergency rocket communications system, to get the orders out in a matter of seconds to the crews. And the crews are in a lot of different places. They may be in airplanes. They may be up in the polar reaches of the globe, or sitting out in a silo at a command and control facility in a rocket field in Wyoming. You have to ensure that they get it, that's why they use redundant systems.

The sixth step is one of the most difficult things to do, if you think we've had problems so far. That is to collect the intelligence and information on what we did to the enemy and what he's done to us; and that, my friends, will be a very iffy business. You hope to do it through reconnaissance aircraft, reconnaissance satellites, Elint sources, etc. It will be difficult to get any sort of communications back through the environment that's going to be existing during that time. But if we don't get that information, then this business of extended hostilities or enduring nuclear strategy is just so much foolishness — if there was anything to it to begin with.

The final step is reconstitution of forces, to carry out whatever remains to be done with whatever you've got left to do it with. And then the entire cycle starts over again. Now that, theoretically, is what strategic connectivity is, and you can see that it's not something the Bell System is going to solve for us, or that any one person is going to solve. It's an extremely complex sequence of actions that have to take place, and have to come about in very short order.

Oettinger. Maybe nothing is happening, so all these schemes in the seven steps are working in principle, and "in principle," you have pointed out, has some iffiness in it. But beyond the principal iffiness, you may have degradation of a piece of the communications network, or a commander-in-chief being disabled, or you may have had a full first strike and these questions of reconstitutability and so on become somewhat science-fictiony. It seems to me from what you've outlined that all these seven steps are enormously scenario-dependent. They depend on the assumptions you make about the nature of the strike — from extremely benign with just the routine ifs, ands, and buts you cited, on to something where the very words seem sort of crazy because there isn't anything to reconstitute on either side. I wonder whether you would give your views, to whatever extent you can, on the details of scenario-dependence, and how much of this is on what level of rationality, in terms of surmise about events that are pretty difficult to characterize.

Ellis. Of course you all recognize that my scenario is a second-strike scenario, and that's what our national policy requires us to assume. If we were only doing the first strike, that's pretty simple by comparison. But that was a response scenario. I'm not really sure I understand your question.

Oettinger. Well, you were about to talk about what we're going to do to improve the system. Improve it with respect to what? What level of scenario are you talking about? How do you make improvement meaningful?

Ellis. Well it's very scenario-dependent, dependent on everything — software not glitching, people not freezing up. What is desired is the same confidence in our connectivity system as we have in our nuclear weapons, and that's something like 99.99% — we know it's going to work. And we know that because of tests and that sort of thing. But there's no way to test a system like this.

Oettinger. It's also a very different kind of system. A weapon is an isolated thing in a definite place, and so on. What you're describing here is widely distributed all over the country and the globe.

Ellis. Yes. And there are a lot of anomalies we don't know enough about. What happens when an airburst is 150 kilometers high, for instance? What kinds of things are going to go wrong with our satellites? What's going to go wrong with our ground-based systems?

We built a great big trestle out at Albuquerque, for instance. We can put a B-52 on that trestle and zap it with 50,000 volts. If we can protect against that, we believe we know our C^3 can stand up. But we don't know it for a fact; we don't know whether it's strong enough. It's interesting: the B-52 is actually a pretty hard bird when it comes to C^3, because it's so old. A lot of its systems are old technology — vacuum tubes. While now we're dealing with chips, and this low-power micro-technology burns out when one lights a match a mile away, so to speak. Well, that's a very difficult thing to comment on. I wish I could be more precise.

Oettinger. Okay. I just wanted to make sure that what was implicit was explicit for everyone in the class.

Ellis. A lot of these things are done by rote. We know, for instance, that the crews are going to react in a certain way if they get a certain message, because we can test them on it, and we do test them. We know how long it takes to fire a missile. We shoot missiles from Vandenberg out into Kwajalein. We know the reliability of a bomber system, we know the reliability of a missile system, because we have tested them, we have dropped bombs, we have done those things. So we know the answers to a lot of things I've talked about. We know how good they are. What we don't know is what people have done to the system. People are the strongest link in the whole system, they are the mandatory link, but they are also the weakest link.

You have all heard about the Titan, and how the new administration is going to take it out of holes because its dangerous to Americans just sitting there. Well, we've had two accidents with that in the last two years, catastrophic kinds of accidents. One Titan blew up, and the fuel leaked out of the other. Both were caused by human error. It wasn't the system; the system is built correctly, but people try to take shortcuts. They don't follow the book. They try to do something in a hurry, or it was Friday night and they wanted to get home — they took shortcuts, and disaster happened. So people are problems. Another example — a controller is sitting in an isolated place and has sole responsibility for monitoring a scope. After he's looked at that scope for awhile, he starts seeing things in that scope. You worry about that. But those are the uncertainties.

I'll just make very general observations on how to improve our current system. I think for the next five or ten years we're going to have to rely for the most part on airborne systems. You have to assume that anything statically located in the United States, or anywhere overseas, if it is fixed, is going to be destroyed. Because if the Soviets know you have it, they also know what part it plays in your overall system, and if it interferes with their plan they're going to destroy it. So we need something that is moving. Just putting everything in space is no answer; ultimately the information has got to get down to the ground somewhere because that's where the decision is going to be made, you assume — unless the president or other NCA is airborne.

There are things we know we can do in the near term. We can harden our satellites, and we have hardened them. We can put all kinds of satellite readouts on our command and control aircraft. We can execute from our aircraft. We can harden our aircraft — one of the E-4s, the big 747s we use for the national emergency airborne command post, has been hardened, and we have reasonable confidence that it is adequate. We're in the process of doing the others. Those are things that can be done, they're state-of-the-art and they're funded. But eventually we're going to have to get back to Mother Earth, because ground basing gives you the most flexibility. Planes run out of fuel, and can stay up only so long; we are going to have to get back on the ground and do the things we used to do and don't know how to do any more.

We're going mobile on a lot of our communications, a lot of our command posts. Ground movement. Mobile command posts will get a readout from our warning satellites and pass it to people who have to be informed. In the 1960s AT&T built hardened transcontinental cables across and up and down the United States. We still use those lines, but over the years the hardness has failed. There are power booster stations along the way, and other gadgets I can't identify, that have to be constantly checked to insure they are still hard and protected.

There are things we can do with industry. The problem with industry today is that it doesn't have the same motivation it had in the 1950s and '60s, because today the government is a lot tougher. It doesn't give industry the profit it used to get, and, more importantly, the competition is tougher. Industry doesn't have to build a hard system to satisfy the commercial user, but when you put a commercial satellite up, if it is hardened so that in wartime it can be used by the military, or if when switching centers are built in the United States they are underground or otherwise hardened, then we can use them. But the government has to set up a system for compensation that commercial companies can live by. There is a model for that: the Civil Reserve Aircraft Fleet. Thus, when an airline buys a big wide-body jet the government will reimburse the airline to refit the aircraft so it can be used to carry tanks and other large equipment in wartime, and then it will pay the airline a yearly fee, including the extra fuel, to carry around the equipment they had to put in the airplane in order to do the wartime job. That's the sort of thing you need in a military-industrial relationship — in communications, and in other areas involved in connectivity. The problem is how to pay for it. This administration has said it's going to spend 18 billion dollars on C^3 over the next six years. That's an incredible sum. SAC and other agencies testified before certain committees in 1980 and Congress earmarked 300 million dollars for C^3I. That was a start.

But a lot has been done in the last few years. Studies have been completed on strategic connectivity. Probably the groundbreaker was the one SAC ran between fall 1978 and early 1979. We had the best brains in the country there, from all the services and from industry. We spelled out the vulnerability of military C^3I, strategic connectivity, and we reached everybody in town except the president on that. That is the kind of effort that is required in the years ahead. We must keep tab on how well we're doing. We must run detailed books. We must do it from an operational, not a systems point of view. The operator is the person who has to use it, and he's the person who makes the best judgment on its effectiveness. We must ensure that the equipment is standardized. Having 18 billion dollars in back of it would help too, but that's just words so far. What we're going to have to do in the out-years is see whether the services put connectivity on a par with service weapons programs in priority of effort and funding. Because it's real easy to put money into C^3 this year and then see it disappear into purely service-related programs later on. At this point I will settle for higher reliability of C^3I.

Student. To what point is it necessary to push funding, considering that under a full-strike scenario nothing will be left of either side?

Ellis. We're looking for deterrence. And if we do our job right, if we've got the right weapon system, and the other side knows it, and we've got the ability to execute it, and we know an awful lot about what he does, then that's how you get deterrence. We put our money there. I want to let the other guy know he's not going to profit by it, and as long as he knows that, he's not going to start.

Student. Do you feel the second strike is synonymous with deterrence?

Ellis. When I went through the seven steps, I was describing a case where we'd already been attacked. One of the most destabilizing things that we and the other side will have to live with is the case where one side knows the other side's C^3 system, or weapon system, is vulnerable. That is an incentive for the side living with that vulnerability to go first.

On another subject: AT&T is critical to our national defense, and I assume it will continue to be strong. The breaking apart of the regional systems is something else. We depend on them too, people like those at Southwestern Bell and Pacific Telephone and Telegraph. Now we are going to be dealing with independent entities who are not particularly interested, or who don't have a whip cracking down on them like Ma Bell is able to do. But maybe competition will make the regional companies even better than they were in the past, because they're going to have competition that they didn't have before.

Student. With the great emphasis on hardening and survivability, don't they too become part of deterrence? Is there an operational definition of hardening?

What exactly does hardening entail?

Ellis. For the operator it means putting into a satellite or an airplane the things that would enable it to live in an electromagnetic environment.

Student. I'd like to get back to where you said people can be your strongest link and also your weakest link. In one of the course papers from 1980 that we looked at, General Paschall said that people in C^{3}I should not only be trained but overtrained.* What is your impression of the personnel staffing?

Ellis. One of our problems is making sure we have a good personnel selection system. We all have that problem. We should always stay in touch with that problem. Because humans design the selection system, maybe we'll just have to settle for second-best! I would say some of the discipline within the military nuclear organizations is about as close to what you want as can be found. They are a body of dedicated people who are professionals you can depend on to do something when they're told to do it — and not to innovate. The last thing you want is innovation. You want them to do exactly what they're told to do, because otherwise someone is going to get killed or hurt or something. I would like to say the system is perfect, but it isn't.

Student. How would you say the Air Force has been doing on junior officer procurement?

Ellis. Much better lately. We haven't talked too much about it, but the experience of Vietnam left a traumatic impact on the military and on the Air Force. Not so much Vietnam itself — that was bad enough — it was the aftereffects, during the 1970s. By the late 1970s it was hard to find the kind of discipline we needed. I think it's a lot better now. One of the reasons we were having problems with acquisition was money. We always hate to come down to money, but that's what man lives by. It feeds the family, it educates the kids. Now they have reached what has been defined as "comparability" in salaries, and we're getting people who want to serve. That's one of the good things. Now we can be selective about who we take in because we are getting people who want to do the job.

Student. One of the things that impressed me was the fact that they finally got the pay comparability back the way it was in 1972 when they first made the implied contract with the Armed Forces that Congress would maintain their comparable level. But when I was a junior officer, my contemporaries and I could not afford to do it. Horror stories were told back then of enlisted personnel being on welfare in various states, which seems to be a little bit out of line if you're going to try to get a volunteer military force. My estimate is that, as you said, the people who are coming in are interested in service to the country, and that we can be selective. The problem is going to be when we get to demographics and we find fewer people from whom to draw, particularly when the economy starts getting better. And that goes back to the expansion problem: budgeting, calling not only for new systems, but the people to man them.

Ellis. The Air Force historically has not had the problems that the Army or the Marines have had and to a lesser degree, the Navy. The Navy is a sophisticated service in terms of equipment, but there is also one thing they do that nobody else likes to do: leave mom and the kids for six months and go out and sit on the Indian Ocean. The Air Force doesn't do that. We stay home for the most part, or at least we're not gone too long when we are gone. So the Air Force has pretty much been able to meet its requirements. But you're exactly right. I'm not sure we're going to get people with the level of training and caliber we want in the quantity we're going to need.

Student. What about the time lag in training? Is there going to be enough time to develop the personnel?

Ellis. Well, historically, we try to input the people at the same pace with the system or the equipment we are buying. It doesn't always work out that way, but that's what we try to do. Additionally, every year we've got a big turnover of missile people who come out of the missile field. Once they've done a tour in the bunker, you have a disciplined professional who will serve very usefully in the command and control field. Now while he may not want to sit in another bunker somewhere else, at least he won't be working on the same instruments. Proper motivation is the key to reducing training requirements.

To sum up quickly, I think it's more interesting now.

*See Lee Paschall, "C^{3}I and the National Military Command System," *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1980*, Program on Information Resources Policy, Center for Information Policy Research, Harvard University, Cambridge, MA, December 1980.

We're in a comparatively undisciplined world today. I guess one of the contributions the university makes is to try to prepare people to bring some discipline to their work, whether it's in military sciences, arms negotiations, or whatever it may be. I think courses like this serve a very useful purpose too. I commend the school for something that gives you the ability to look into a much wider range of topics than you normally would get into.