INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

C^{3}I and Crisis Management
Stuart E. Branch

Guest Presentations, Spring 1984
Richard S. Beal; Stuart E. Branch; Leo Cherne; Hubert L. Kertz; David McManis; Robert A. Rosenberg; James W. Stansberry; W. Scott Thompson

February 1985

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	*Managing Director*
Anthony G. Oettinger	John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
I-85-2

C^{3}I and Crisis Management

Stuart E. Branch

Mr. Branch is Deputy Assistant Secretary for Communications in the Department of State, and he also serves as a principal member of the National Communications System and of the US Communications Security Board of the National Security Council. Earlier assignments include service with the Department of State as Chief of the Communications Facilities Staff and as the African Operations Officer. He then became Communications Officer to the American Embassy in Saigon and afterwards to the American Embassy in Mexico City. Upon his return to Washington in 1973, he became Chief of the Department of State's Communications Center Division, a post he held until 1977. He then served as the Executive Officer for the Office of Communications until his appointment to his present post in July 1978.

I am pleased to be here. (Someone said it was going to be fun, so don't disappoint me.) I would like to begin by running you through a few slides put together by the Office of Communications, Department of State. Since I am no longer Deputy Assistant Secretary of State for Communications, I should underscore that my views do not necessarily represent those of the State Department.

I believe the slides will explain the responsibilities of the Office of Communications, its authority, and what we do at our embassies. Then we can explore areas of interest that might strengthen the national security of the State Department's communications system, particularly international communications. This area has received a lot of attention in the past and in this administration. The Carter administration recognized the problem and issued Presidential Directive 53. Although not much happened in the implementation of that directive, it did stress the need for a national security communications system that is restorable, interoperable, and survivable. The directive had its roots in the rewrite of the Communications Act, begun during the Carter administration and proposed several times in different committees in Congress. Some of you probably know a good deal more about it than I do. There was concern on the part of some of the national security elements of our government that the rewrite of the Communications Act did not adequately address our government's national security telecommunications needs.

One of the previous speakers, Bill Odom, was a senior military advisor during the Carter Administration National Security Council, and he chaired a meeting of civil government agencies. Most of the civil government agencies and the National Communication Systems principals were represented, perhaps the Armed Services as well. Odom was searching for the civil government agencies' views of that proposed rewrite of the Communications Act as it related to national security telecommunications. He asked, as I recall, three questions. He said he didn't have a lot of time, he wanted only yesses and nos, and he wanted to go around the room. Did the rewrite of the Communications Act, as proposed, adequately address the survivability of the nation's telecommunications systems, and if it did not, should it? We went around the room on the yesses and nos, and then he asked the same thing for restorability and for interoperability. The consensus was that on all three counts, the current rewrite did not adequately address the factor, so Presidential Directive 53 followed on the heels of that.

The Directive charged the National Communications System to be the executive agent for implementation of that Presidential Directive to ensure that our national security communications system indeed was survivable, restorable, and interoperable.

I want to come back to PD 53 because it leads to National Security Decision Directive (NSDD) 97, the National Security Telecommunications Advisory Committee, and some other actions that are much more current than Presidential Directive 53. Now to the slides.

I would like to emphasize that the communications system we operate at the State Department is really in support of the foreign affairs agencies. More than half of the information flowing from our foreign service posts is addressed to other government agencies and departments, and not to the State Department. It is this single network, this diplomatic network, that supports our embassy personnel. About 17 percent of the people at the embassies are State Department employees. The rest of the people at our foreign service missions are members of the other foreign affairs agencies, or agencies having an interest in foreign affairs: Agency for International Development (AID), U.S. Information Agency (USIA), Commerce, Agriculture, Defense Attachés, etc.

We operate overseas through the Diplomatic Telecommunications Service (DTS). The DTS is overseen by a senior policy board with representatives from industry and government. The chairman of the policy board is Dr. William (Bill) Baker, former Chairman of Bell Laboratories. The board guides us in long-term planning.

Later, we will discuss the use of this diplomatic telecommunications system as a means of avoiding confrontation or in cessation of hostilities when there is a confrontation. I would like to remind you that the ambassador is a personal representative of the President, although we tend to think of him as a member of the State Department. So when we start thinking about communications between heads of state, let's remember that that ambassador is the President's man on the scene. That may have some bearing on some decisions in terms of how we improve our interpersonnel communications capability to avoid hostilities. Those of you who have telecommunications backgrounds might view our system as essentially a traditional Telex communications service, but, in fact, it is an aggregate of many varied services. We're responsible for the mail, both classified and unclassified; for voice radio, including very high frequency (VHF), high frequency (HF), and ultra-high frequency (UHF); and for overseas telephone systems, operators, and receptionists. Additional communications responsibilities include such services as file management at the embassies. You might want to make a note of secure voice because it will play an increasingly important role — as will electronic file management — in the protection of information and protection of individuals who are cooperating with our diplomatic personnel overseas. Our system is based on the traditional technologies for word processing, file management, and data processing, but it is adapted and certified for the handling of classified information. We also have a program to add a fully secure automated office system in the offices of the Ambassador, the Deputy Chief of Mission, political counselors, and economic counselors. This new electronic file management system allows us to process classified information without being concerned about it being compromised. The electronic file management is local in nature. We have only limited capability for a distributed data base. While we are planning a network based on that concept, for the moment our electronic file management can only capture the information flowing to and from an embassy, store it electronically, and retrieve it on those same terminals.

Student: So would you call it an electronic mail system?

Branch: I keep asking, "What is electronic mail?" We call it telegraphic. We are linking that system with our telecommunications network, so direct access can be provided between a terminal in the political counselor's office in Bonn, Germany, with terminals in the Bureau of European Affairs in the State Department. The capabilities are very limited at the moment, because the system must be fully certified for handling classified information. As the use of fiber optics increases, we can expand much more quickly. So, yes, although limited in capability, it is an electronic mail in the sense that it is an interactive system with remote terminals.

Student: Would you say that the local electronic mail, say, in the Bonn embassy, is a sophisticated electronic mail system?

Branch: Yes, it uses the Wang Alliance software, and if you're familiar with that, then you know what features are built into it. In addition there is the capability to access the electronic file storage device, which is an adjunct of our communications terminal. Thus, in addition to access to the central processing unit of the Wang system, there is also a high-speed data-link extended to the electronic file.

Let's return again to our overseas operating environment: we serve about 250 diplomatic posts, embassies and consulates — the number varies depending upon political factors and changing relationships with other governments. An embassy staff may consist of representatives from nearly 50 foreign affairs agencies.

When you think of the State Department, you don't think of command, control, communications and intelligence. It's sometimes difficult to relate C^3I to a diplomatic mission. I would suggest — and hope to get some reaction from those of you with military backgrounds — that the State Department's communications system is as much a piece of that worldwide military command system as are the defense elements, and that it has the potential of playing as much a role in command, control, and communications as do a number of the military systems.

The center circle in figure 1 represents the automated terminal stations I've been describing and shows how the information flows from posts. At the extreme left and right are embassies and diplomatic missions. Information flows from them to nodal or relay points, then back to a central point in the State Department. The interaction of defense networks through the Pentagon is shown on the lower portion directly off the bottom of that ATS circle. You can see the Bonn BAX relay, and directly below it, Pirmasens, the military facility that is also a part of the military network.

At any point on this chart, communications routing can be done. It consists of finding the point at which you can most quickly enter information into the defense network, automatically restructure it into the format that the defense network can deal with, and move that information to its destination. Once the information reaches that center circle in the State Department, a similar network reaches out — electronically secure — to almost all of the government agencies in Washington. As the information hits that circle, one of two things happens. The computer takes a look at it and recognizes that certain organizations need to have this information. The designated center receives the information, queues it, and sends it automatically over the circuits to those centers where it is read and distributed within those agencies. The computer that reads the information tries to determine who needs to know whether it has been sent or received. It routes 58 percent of the information automatically, without human intervention in a distribution format. Of course, there are still a number of tasks that remain the responsibility of the information analysts.

Certain of the factors driving State Department activity change significantly over time. Natural disasters of course do not, but terrorist activity, embassy seizures, international hijackings — these fluctuate in a significant way. We must respond to events such as threats to U.S. personnel by mobilizing communications systems and trying to assist in negotiations. We might want to come back to these events when we start talking about how the government deals with war avoidance or crisis management.

The Beirut Embassy bombing is a crisis situation you all are well aware of. We lost our communications center in that bombing. As at most, if not all, of our locations, we had some off-site capability. Our off-site communications capability could handle only a limited amount of information, so we augmented it with certain tactical satellite systems. We were back on the air within 24 hours with full capability in a different location.

When the State Department talks about tactical satellite systems and quick response, the military folks most often think of a system deployed via air, as would be done by the White House Communications Agency. So many times in our environment, however, you're not going into a place where you have a landing strip. You don't have a controlled environment; you have mobs in the street. You don't have emergency power, you don't have space, you don't have security. You don't have air transportation or any of the other transportable systems available to the Army and the Air Force Commands.

The first time I really ran headlong into these circumstances was when we had our first problem in Iran. The Under Secretary for Management wanted me to put together a transportable package and get it to a consulate in Iran so it would have a secure, increased-capacity communications capability. I had to go back and tell him I couldn't do it. I just couldn't get in. I couldn't get there from where I was with the equipment we had. So he went to the military, and they said, no problem, we can do that

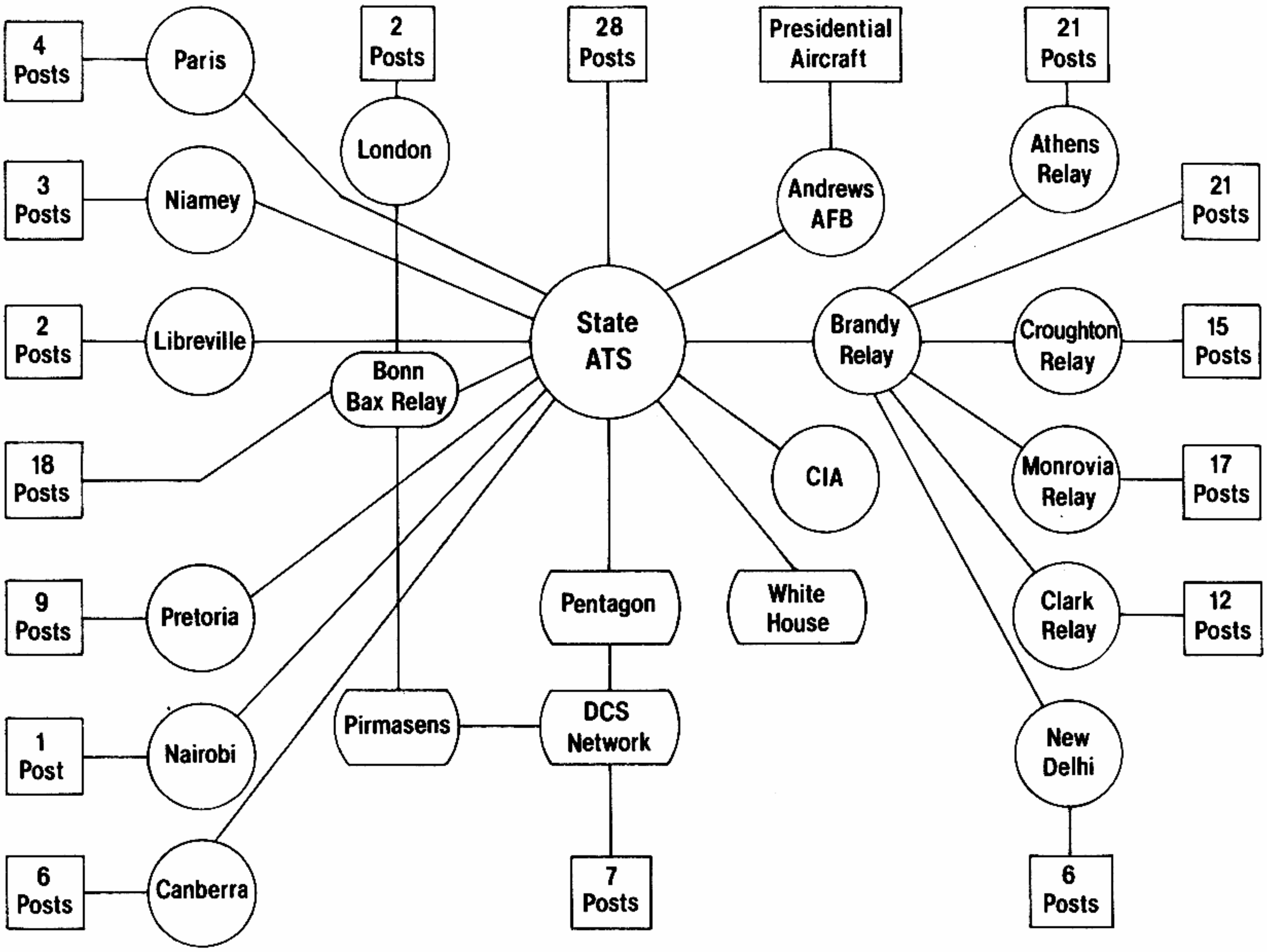

Figure 1.
Department of State DTS Network Program

for you. Their system turned out to be a truck, a trailer, and five guys in uniform, but we couldn't land that equipment at that site. There wasn't an airstrip that could handle the weight. You had to run through town with the mobs demonstrating; if you did reach your destination, you would find it was both a consulate building and a residence — the guy had his bedroom and office in the same building. He didn't have any place to set up communications gear like that. So in the area of quick-response, transportable systems, we now have a capability of transportable satellite equipment we didn't have at the time.

On the other hand there is Grenada, where we used a transportable satellite terminal. We had a member of our staff go in with the first wave, and we set up on one end of the airstrip while the military was still hitting the other end. We had to provide the communications out there for a long time before we set up a permanent capability.

We encountered a similar incident in the Sudan. We had a hostage situation involving four Americans. We brought in a tactical satellite terminal and secure facsimile equipment. We set up near the airport, and we were able to transmit maps of the position of the aircraft, the flightline, etc., to headquarters in the Department, where they had a command center. They were able to negotiate successfully the release of those hostages. Again, that was using tactical systems. As a footnote I recall that we called a fellow at 8:00 p.m. in the middle of dinner and asked if he could go to Sudan in the morning with a tactical satellite terminal and set it up. No problem — he had it packed up and he took off with it.

The Office of Communications also provides support when the Secretary of State travels out of Washington. When he moves, we move with him. But unlike the White House Communications Agency, we draw from our normal staff, including embassy staff. We bring those people in or we draw from Washington.

Student: What kind of duplication is there between your office and the Defense Department? Does it have its own set of equipment?

Branch: No. We provided the communications capability for the team that went in to negotiate the release of those hostages and the Defense Department used the system. We provided the command and control link for the ground team that was trying to deal with the situation.

Student: Is that usually the case? In Grenada, for example?

Branch: In Grenada, the Defense Department provided their communications with defense elements, but we provided the command, control, and communications for the diplomatic effort. There were other communications capabilities out there, but they were in support of specific missions, such as defense and intelligence. In that situation, the diplomatic channel supported the diplomatic efforts. But there is much less duplication than you would imagine with so many foreign affairs agencies represented at an embassy. The Sudan situation was a little different because we weren't at an embassy, but it's not unlike what you would find if we had gone to an embassy or a consulate. Generally speaking, we are the landlord and the others are the tenants, and we provide administrative service. There are some exceptions, but they are very few. You will almost never find any of the other agencies with their separate communication centers, people, circuits and all of that. This role of providing communications for the foreign affairs community is regularly reviewed by Congress in the budget process. One of the concerns for Dr. Baker and the DTS policy board is to deal with that very issue, to make certain we don't have too much overlapping of responsibility.

Some of the pressures that cause change in the foreign affairs communication system include executive branch initiatives, a changing regulatory environment, new technologies, and increasing consumer demand.

The changing regulatory environment — be it domestic or overseas — is a force that the Office of Communications never had to be terribly concerned about in the past. Our diplomatic missions and our communications flow are pretty much protected by the Vienna Convention in terms of movements, transmission, and receipt of information on the part of sending and receiving nations. But changes in the regulatory environment are beginning to impact our system in a way it never has before. I don't pretend to be an expert in any of these areas, but I wonder if there is not at least the potential for change in our arrangements with various governments considering some of the actions of the Federal Communications Commission (FCC), the reactions of the PTTs including volume-sensitive pricing for transborder traffic, and our increasing use of interactive terminals. I also think we may soon need bilateral or multilateral agreements about information flow between the U.S. and other governments.

A lot of our present information flow is between communications centers, between embassies, or between an embassy and Washington. In the last two years we have been trying to get closer to the user, and this is something I want you folks to think about and maybe someday share some thoughts with me. I'm convinced that we will be successful in moving more information faster than ever before, and getting it closer to the user. That's "ho-hum" technology, even with the requirement to make it secure. It's a function of how many people we can throw at installations and logistical support. However, my concern is this: having done that, I don't think we will have accomplished a thing for the decision maker. If anything I think we're going to frustrate that process. If we're looking at command, control, communications, or the National Command Authority and we're talking about avoiding hostilities or a cessation of hostilities, and all we're doing is building the pipes bigger, have we really promoted our national security?

I am asking that question. I don't have the answer. I believe the answers will be found in the environment of academe, not in ours. You have an opportunity to examine and study things in ways that we who are building and operating the systems don't.

I'd like to ask you some rather basic questions. The format of the information we process and transmit today is the same format we used 30 years ago when I came into the foreign service. We had a different name for it, but it's pretty much the same thing: we break information up into segments. Why do we break it into segments? Because of the nature of the communications network. But the end users still get that same information. A 16-page, week-old telegram gets to its recipient's desk today the same way it did 15 years ago. We've improved it: we put a subject line on. We told them they must use a subject line. Having said that, most telegrams coming in from the field identify subjects in a way that is not always adequately descriptive. So my question is: Why do we present the information that way? Why can't we take better advantage of technology?

Also, why do we need to send every piece of information? If we have real-time file retrieval, why don't we move information differently? Why don't we move summaries? Why don't we move numbers? Why don't we let the user tell the machine what he wants to see and not see? Those are things we've got to take a look at. Let me stop here for questions.

Student: Could you tell us something about the current thinking of informing a decision maker? Have there been any initiatives recently in the Department? Is there any work being done?

Branch: In terms of answering some of the questions I asked we have done almost nothing. We started discussions with MIT to organize a group to help us in that area. By the time I left, we had not gone anywhere with it. Now, in terms of informing the decision maker, we're moving information to him very rapidly using all kinds of communications capabilities. But as far as facilitating the decision making process, we haven't gone anywhere with it.

Student: I'm a little leary of technical solutions in certain problems. If I could explore this question about assisting in a decision making process — what are the users asking for that you have difficulty providing?

Branch: Users are just beginning to experience the problem of too much information flowing from embassies to Washington, or from Washington to embassies. It is very difficult to sort through that and find out what is important, what's timely, and what ought to be on that desk. We are building the technical capability out there that's encouraging movement of information, and it is moving. In fact, in some cases, it's looping. I spoke to one ambassador who mentioned this problem. He said, "I'm getting too much information. I'm even getting information we generate! Our political counselor writes a report that deals with military activities, sends it to Washington, where it is sent to the Defense Department, where it is sent back to us because it divulges military actions here in this country. And the report originated here." That's an example. I'm not suggesting there's a lot of that, but it's an example.

Student: So you suspect that users could provide some criteria that could help design a system.

Branch: Yes, I think they could. I don't know that you're going to design a total system or that you're going to deal with the total information flow, but I believe that you could handle that information differently and let the user interact with that system more directly. For instance, if a political counselor is working on the downing of a Korean airliner and doesn't want to deal with anything else that day, why are we sending him all kinds of other information? Instead of relying on the user to sort it all out, why can't we use technology to give him only that priority information and file the rest for him to review later?

Student: With the available technology, I'm surprised you can't do some of the things you've mentioned. For example, you've got a system of tags, you've got other ways of organizing the information. You have terminals in the front offices of the bureaus, so I don't know why those terminals couldn't be put in the individual offices, so that if the guy needs all the information that's coming in with a certain tag and a certain subject, he could filter out everything but that.

Branch: The technology is there in pieces, but the networking has not been done. I think it should be done incrementally — build on the installed base, then take a look at a large universe of information an officer might want. You're right, a lot of the technology is already here.

Student: Stu, I just want to comment on something I noticed in 1982 when I was working with Phil Habib, who was in Lebanon for the Palestine Liberation Organization (PLO) withdrawal. For years, ambassadors have been hollering at us for centralizing information in Washington and taking away their decision making role. With the use of the secure voice Tactical Satellite Communications (TACSATCOM), Habib was able to reverse that, and he did exactly what we're saying. Maybe we ought to look at that more carefully. He went back to Washington personally and made the decisions, because he was out there, the tanks were rumbling and he needed decisions made in a very timely fashion. Do you think we may have a decentralization of authority and control in the future based on the use of technology?

Branch: Well, there are people who like to think that that will happen. My feeling, though, is probably not. What you were witnessing was the *personality in charge,* not so much technology. Habib was the kind of fellow who would have packed up and gone home if he weren't calling the shots. Maybe we need a few more ambassadors like that who recognize they are representatives of the President. Having said that, you can't circumvent the National Command Authority, whatever that means, and so they're probably going to go the other way. In fact, we're going to see more and more centralization of the formulation and the execution of foreign policy. I don't know if that's by design or if it's accidental. I think that technology is encouraging centralization because information can flow back and forth.

It's not just in the State Department or the diplomatic service — the Washington managers are involving themselves in the decision making process as they never have because they are on a much shorter leash than ever before. We used to beat that by saying, "I can't hear you," or "I didn't get that memorandum." Now you've got them right on the other end of your system. I think that concept is contributing to this shift of centralization of the control to Washington, but I think there are also a number of other things that cause it.

Clearly, the interrelationship of issues across our government demands that information be shared, and that inputs from the defense, intelligence, and other sectors of our Executive Branch be factored into that decision making process. Also, it limits the occasions in which an ambassador can act on his own and then report back after the fact. Of course, the argument continues about whether there's too much or too little control from Washington, whether the coordination is good or bad.

Student: Could you comment a bit more on what State is doing about this problem of increasing information?

Branch: They are planning to proceed with an examination of the problem, whether that's with MIT or with another group is not clear at the moment. I think that we will see the application of available technology to monitor the data stream and to provide distributed storage and retrieval. There will also be a fresh look at whether we can continue to structure, present, and move information the way we do. I think the department will continue to examine these concepts, and then try to use the present equipment to handle information.

I mentioned the Presidential Directives regarding national telecommunications and how they came about, and that implementation responsibility went to the National Communications System. It was concluded, however, that as a government entity it alone couldn't do a great deal to improve the system's survivability, restorability, and interoperability. That's because some 90 percent of the communication system the Defense Department depends on belongs to the private sector. So the next step was to involve the private sector in the process. The National Security Telecommunications Advisory Committee to the President was formed. It consists of 30 chief executives, representing the satellite, data processing, and telecommunications fields. Tasking for the National Communications System, as contained in Presidential Directive 53, was primarily addressed to domestic communications systems, so it was difficult to see a concern about our international communications. When Presidential Directive 53 was rewritten as National Security Decision Directive 97, it specifically incorporated language addressing the international side and asked the State Department to study and manage international services. The National Communication System remains the executive agent but the State Department had agency responsibility for meeting survivability, restorability, and interoperability criteria. The Department asked the National Security Telecommunications Advisory Committee to put together a task force to examine international telecommunications and give us some thoughts on how we could make the international communications commercial operations more survivable, more interoperable, and more restorable. That task force was put together with about 13 representatives of industry. Part one of their report was issued in April 1984. It was sent to the White House and accepted. Part two was completed later in the year.

The report includes recommendations that you would expect: greater use of commercial satellites from embassy premises as opposed to terrestrial PTT facilities (recognizing that this would require a lot of coordination with those governments, some regulatory issues, and some legal issues). Also suggested are ways to build in greater redundancy in the communications between the embassy and central offices or earth stations. We should also improve the restoration priority assigned to our critical circuits.

One of the concerns we had was how the divestiture of AT&T would affect our embassies in Washington and overseas. When Bill Hillsman was director of the Defense Communications Agency he used to say who do we call after divestiture? We call AT&T now; who will we call to restore our communications? Think about that a minute — who do the embassy communications officers in Washington call? Are they going to work their way through this maze? We put together an organization called the National Communications Coordinating Center, under the Defense Communications Agency, and that's supposed to be the place where we have industry and government representatives jointly operating. If you have a serious problem, you call there and that's where it comes together.

Oettinger: The one remaining problem there is that nobody has figured out how to pay for that.

Branch: That question was brought up earlier, and it's still being asked.

Oettinger: As of last week it hadn't been resolved.

Branch: When AT&T provided that service, it was covered by the base rate. Included, but not specified, were the costs for providing survivability, interoperability, and restorability. What portion of the total bill I don't know, and in what bills I don't know. But you're right, cost is an issue.

Separately, the President signed a new Executive Order on national security telecommunications in April 1984. As you examine what we do with the nation's telecommunications system to assist in war avoidance or in stress situations, I think it's important to understand that there are at least some relevant steps already being taken within the Executive Branch. The subject of this recent Executive Order is the responsibilities of the various executive agencies for national security telecommunications. If I may, I'll read very quickly a two-page fact sheet on it. It was issued on April 4.

> The President today signed an Executive Order which consolidated the assignment and responsibility for improved execution of telecommunications functions which support national security and emergency preparedness. The domestic and international telecommunications resources of the United States, including commercial government and privately owned services and facilities, are essential elements in support of national

> security policy and are vital to emergency preparedness. A survivable domestic and international telecommunications infrastructure with the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security is essential for national security and emergency preparedness requirements in all circumstances including those of crisis emergency. The Executive Order establishes a framework for (1) the planning, development, exercise, and capability to satisfy national security and emergency preparedness telecommunication needs of the Federal government, and (2) providing advice and assistance to state and local government, private industry and volunteer organizations on request regarding their national security and emergency preparedness telecommunications requirements. The order establishes a planning and management framework for all conditions of crisis or emergency, including international crises, attack, recovery and reconstitution, and the entire range of civil preparedness emergencies such as earthquakes and hurricanes. The order also specifies the national security/emergency preparedness telecommunications roles and responsibilities among the Executive Office of the President and the various Federal departments and agencies. The order establishes the National Communications Systems to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in the discharge of the National Security/Emergency Preparedness Telecommunications function.

The National Communications System has been in existence since about 1963, but it is as a result of a memorandum, as I understand it, and not by an Executive Order.

Oettinger: It was a John F. Kennedy memorandum in response to his inability to communicate with South America at the time of the Cuban problem, and it has been sort of in effect ever since.

Branch: So this Executive Order institutionalizes the National Communications System. I'll continue:

> The National Communications System consists of the telecommunications assets of the entities represented on the National Communications System; a Committee of Principals; and an administrative structure consisting of an executive agent, and a manager.
>
> The NCS Committee of Principals is composed of representatives of those federal departments, agencies, and entities with significant national security/emergency preparedness telecommunications responsibilities. The NCS will assist in planning, and the Executive Order assigns specific planning, management and oversight responsibilities to the National Security Council, the Director of the Office of Science and Technology Policy, and certain key federal agencies including the Departments of State, Defense and Commerce and the Federal Emergency Management Agency.

I think this is a terribly important document with regard to our national security telecommunications assets in the context of avoiding hostilities, restoration, cessation of hostilities, or crisis management. Whether or not it will be effective, it certainly, in my judgment, strengthens the NCS in a significant way. Whether or not the NCS has the inclination or the budgetary or personnel resources to carry out its responsibilities or is successful in getting resources is quite another matter. Certainly the authority is there. The authority is there for every government agency to address the national security dimension of its telecommunication plan. But whether or not the agencies have the wherewithal in terms of the budget to implement this Executive Order is an open issue.

My personal observation is that while there is serious concern about the capability of our national security telecommunications assets to accommodate the stress conditions you have examined, and while there are many advocates within the Administration for improving our capabilities — witness this new Executive Order — there seems to be a gap between what the policy is and where the resources are to implement it. I'm not suggesting that we cannot revise our thinking, revise our planning, and take national security and survivability into the planning process as we design our systems. But a program of this magnitude is going to span administrations, and it is unclear whether there is a national commitment to this philosophy that would carry through administrations and provide the funding necessary to support it over the long haul.

It's common to measure the cost of system acquisition, and maybe even system activation, but it's not as common to measure carefully the cost of maintaining this kind of capability over the long haul — the personnel, training, logistics, facilities, and updating. It's a tremendous effort to keep abreast of the state of the art. If you build a system for emergency purposes, at what point do the funds dry up because the more pressing need is day-to-day? Who makes that decision? I do not in any way suggest that we don't examine emergency needs or fold them into our design process, but I'm not certain that we have accurately measured the total cost of implementation.

Oettinger: One of the reasons may be that some of the words, "restoration" and so on, have been linked to the apocalyptic Single Integrated Operational Plan (SIOP), trans-attack, post-attack nuclear, etc., and most of the world, most of the time, is in a lesser state of crisis, like somebody burning up an embassy.

Branch: Good point. That's why I started by outlining our national security communication system, an international network used to deal with crises or stress situations.

As I noted earlier, the network is at some 250-odd locations. It's there for a daily operational need. It is secure. It is already handling a good deal of national security information. If indeed there is a need for this additional capability directed by the latest Executive Order, I feel it must be built on what exists. My concern is that a lot of the recommendations being made do not consider what is in place today.

Now if you build a separate communications capability in addition to what is out there, are you building one that you're going to be able to guarantee for the long term? Will it work when you need it? My experience to date has been that if you want a system that's going to respond in emergency situations, it ought to be the same system you're using to meet daily operational needs. Or it ought to be built on, or integrated with, the same system used in a day-to-day operation. The hardware to meet an expanded crisis requirement is a carbon copy of what is in place today. Thus, the logistics chain is the same for that segment of the network intended to meet stress situations as it is for that which is meeting the day-to-day need. Your training is no different, nor your assignments, nor your support. What happens in a stress situation when you move a technician from a regional center into a stress post, if when he gets there he finds out he doesn't know that equipment? He doesn't have the tools, training, or the test equipment. What do you do with the cadre of people you trained on that equipment? Do you expect them to maintain it all? Where do the multiple skills you expect these people to possess come from? Where do you recruit, train and retain those kinds of skills in this environment, competing with the private sector? In my judgment the two systems need to be fully integrated.

Oettinger: Could you comment on the hot line in that context? How dependent or independent is it of day-to-day kinds of things? That's the sort of concrete example for which there is some reasonable history and some public domain treaty language.

Branch: The hot line is an example of a system that works well. It is superb in terms of reliability, availability, capability, and it is not part of what I just described. Having said that, a hot line is a single point-to-point link and it's an exception in this world. It does not address what one does in a Falkland Islands situation; it doesn't take care of negotiating with the British or with the Argentine government in a stress situation. It doesn't help you in any other location. But let's go back to the Moscow hot line. I think you have the history on it. If you don't I've made some copies of an article recently published in *Signal Magazine*, which is the trade journal of the Armed Forces Communications and Electronics Association. Dr. Jon Boyes, president of that organization, wrote on crisis stability and C^3I, and it's his commentary on the Moscow hot line specifically, and his thoughts on what we ought to do. It captures, I think, rather nicely the history of how that came about and where we are today. First of all, I would suggest that if the diplomatic system had been responsive in the first instance, we might not have had a hot line. If there had been in place the kind of capability I just described, and Kennedy and Khrushchev had been communicating on a real-time basis, and if each could have expressed clearly to the other his intentions, then I wonder if after that situation subsided whether there would have been any discussion of improved communications. So I would suggest that while it's in place and it works, it grew out of the inadequacy of the day-to-day system. By the way, I was in Moscow at that time and I can tell you that it was inadequate. We were working at 50 baud which is about 67 words a minute, and we were working through the Moscow PTT.

Student: I'd argue that that kind of system is inevitable when you have two bureaucracies building up on either side. It's like two CEOs who need to talk to each other to get the bottom line on some big issue. When you've got these two organizations built up on either side, certain bureaucratic forces will not allow the creation of an efficient system.

Branch: Would you go so far as to acknowledge that there's room for both? That's why I say you ought to have a much more survivable and responsive day-to-day system, and that if there's a need for a head-of-state system it would be purely head-of-state for the most restricted kind of communications.

Student: Oh, yes.

Branch: My concern is that there's a tendency on the part of some to look at a head-of-state communication system and then start "wiring it for sound." You have the attitude that; "what you really ought to do is hook it into defense, and hook it into here, and hook it into there." Soon you'll see an expansion and a layering of a network in a way that doesn't reflect the organizational structure at all. I'm concerned about what that means to our national security in the longer term. I'm concerned we will create a different kind of a problem altogether — that is, a circumvention of the existing organizational structure. Where's the Defense Attaché Office; where's that input into that decision making process? Where are the other agencies with knowledge of the host government? Are their views being reflected in that hot line if that hot line is not terribly restricted in the kinds of data sent over it?

Student: What is the date of that *Signal* article?

Branch: March 1984. It talks specifically about the Moscow hot line, and I'll take a moment to review aspects of it. It had its origin in the frustration of Kennedy and Khrushchev. Notwithstanding photographs of a President on the telephone, there is no voice communications capability in that system. It is a low-speed, record, teletype communications system, and when I say low speed I'm talking 100 words a minute. It is point-to-point, secure. There is a test message generated every two hours, maybe once an hour — non-political in nature, selected from periodicals, transmitted from this end to the other end, received in English on the other end, and received in Russian here. It has had operational live traffic, if you will, but not often.

There has been concern on the Hill, voiced by Senators Nunn and Warner and the late Senator Jackson. Nunn and Warner would like to expand the networking capability to include joint military command centers, other kinds of terminals, on this end and the other. The most recent initiative on the part of the Hill was in the U.S. Department of Defense Authorization Act of 1983, which directed the Secretary of Defense to study possible initiatives for improving containment and control of the use of nuclear weapons, particularly during crises. After that examination was completed, the proposals that came back included adding a number of capabilities to the Moscow hot line. It included the creation of a bilateral U.S.-U.S.S.R. joint military communications link, the establishment of high-data-rate links between the governments and their embassies — that's back to taking our existing network and expanding it — and an agreement to consult with other nations in the event of a nuclear incident involving a terrorist group. This report was endorsed by President Reagan in May of 1983 and these proposals along with others are now being discussed between the Soviets and the Americans.

The Defense Department study took note of other communications techniques such as voice and video, but dismissed them on the basis of possible misunderstandings, misinterpretations, or adverse reactions that could flow from their use. The study contained a lot of recommendations concerning what we ought to do. We culled out many of them because of those concerns. We settled on three things: a joint-military-command-center to joint-military-command-center link, improved embassy-to-embassy communications capabilities, and the addition of a secure facsimile for the hot line.

There is more information in the *Signal* piece. It addresses the very issue you're looking at, in a very straightforward manner. We are still negotiating with the Soviets on upgrading this facility. Although I have left government service I have been retained by the Department as Deputy Chairman of the U.S. negotiating team. We'll be going to Moscow for our third round of discussions with the Soviets on those three areas of improvement.

Now, while a lot of people both within our government and without are recommending all kinds of changes, trying to be responsive to the Hill and to others, and responsive to their own beliefs that we ought to have improved communications, too often they don't consider what the reaction of the other party in the negotiations might be to such recommendations. I must tell you very candidly, and I don't think it's sensitive, that the Soviets have not been terribly responsive to anything other than the addition of the facsimile to the hot line. When we first met with them and proposed these areas of improvement, they made it very clear that they were only prepared to discuss operational improvement of the existing hot line. Their words were very, very carefully chosen.

Oettinger: Almost a year ago, direct-dialing into the·Soviet Union became impossible. In the aftermath of the Polish situation, they knocked off direct-dialing. But let's go back for a moment to the period just before Solidarity, martial law, etc., when the best way to reach any dissident in the Soviet Union was by dialing him directly on the telephone. Now in a situation like that, why is there concern on either side about any major change? I mean the President of the United States could pick up the damn phone and dial and say, "Hey, comrade." Why are there arguments when there are alternatives? What purpose does the hot line serve that couldn't be served by simply keeping a bunch of lines open through the normal process any commercial enterprise would use?

Branch: Well, there's no desire on the part of our government — I can't speak for the Soviets — to have voice communications between heads of state. At this stage, our government still wants to record communications. The kinds of situations the hot line would be used for are clearly identified in advance and very rigid in their application. So first, it's not a case of seeking voice communications with the head of state. Second, a standard commercial system is not secure. One might argue that if the chips are down it doesn't have to be. On the other hand, you're trying to avoid a confrontation and not add to the problems with third parties having access to those discussions and taking unsanctioned actions.

The third point I would make is that while that capability is here today, it might not be in a stress situation. Evidence what happened in Poland. Where was the press in Poland? Where were commercial communications in Poland? Up until that moment we had no trouble communicating with Warsaw. It was one of the places we could get to. What about Iran? If I had to pick a country in this world where we were solid, it was Iran. Two years before that place blew up, would I have been successful in getting resources to build survivable communications in Iran? My guess is, probably not. At the same time, when it blew it was very difficult to pick up the phone and work with that embassy.

Now, having said that, and in support of the international record carriers in this country, they did everything possible to provide communications to and from those embassies. And they were most successful, I must tell you. Unusual circuit routings were used, and we had voice communications with those embassies in many periods, thanks to the international record carriers. They acted on nothing more than a telephone call from the two men expressing a need, and they simply met it. There was no business of contracts and all of that. We got the job done, and they were most responsive. Now there's something I'd like to share with you. I'm not selling the stock of the private sector, but I have to tell you I have been most impressed with the responsiveness and concern of the private sector in the area of international telecommunications for our national security needs. It has been most responsive in the dealings I have had, and I was certainly pleased that a communications manager with the government would be able to find that kind of responsiveness.

Oettinger: For those of you who questioned why we chose today to hand out A'Hearn's interview with Hornig on the Northeast power failure,* it is on this very point.

Branch: I'll give you another example, if I may. Islamabad. We had 200,000 demonstrators on the streets; our people were holed up in the communications center. The dissidents had set the building on

*Francis W. A'Hearn. *Northeast Power Failure*, and *Lyndon B. Johnson: An Interview with Donald F. Hornig, June 30, 1983.* Program Information Resources Policy, Harvard University: Cambridge, MA: October 1984.

fire. We had heat so great that the tiles were popping from the floor. We destroyed all of our classified information and all our cryptographic information while we had 130 people in a burning mission — and our government-owned communications were not working.

We had 15 dissidents on the roof with automatic weapons, and our communications antennas were on the roof. They took the antennas, just for something to do, and ripped them off and threw them over the side. They were firing automatic weapons down the air conditioning shaft, which led directly to the communications center. We had an emergency egress from the communications center, but as in most instances, that center was on the highest level of the embassy, so the egress was the roof. In that situation, I was in the command center in Washington. We were communicating between the Assistant Secretary responsible for the geographic area, and directly with those personnel at the embassy. We were using commercial telephone circuits made available by the private sector, which kept those circuits up.

So when I talk about strengthening international communications, I mention repeatedly the commercial portions. We have a policy in the State Department to have a multimedia network so we're working both U.S. government-owned as well as commercial facilities. We're trying to strengthen the commercial side, and at the same time have in place government-owned capability.

There are some things we could have done, and again, I want to go back to the funding and the commitment for funding. After the violence, we examined the situation in Teheran, and we examined the situation in Islamabad. We tried to develop a plan that would help protect our personnel and our facilities at embassies abroad. We developed a program, we brought it through the Office of Management and Budget, we brought it to the Hill, and we got the funding necessary to enhance our security posture at our embassies to protect against mob violence. I'll make that clear. It was not a broad mandate to do everything. We said there is a new threat to our personnel, and there is a new threat to our classified information. It is mob violence. We experienced it in three places because we had a problem in Libya at the same time. We brought that program forward and we had it funded.

Our added improvements to our communications included the electronic file storage device I mentioned, which picks up all the classified information flowing in and out of that embassy and puts it into electronic storage. It gives us the ability to store an almost unlimited amount — at the moment it's running about 15,000 documents — and to destroy it immediately. Take a situation like Islamabad, with temperatures running the way they were and 130 people in the center. The last thing you need to do is crank up an incinerator and start trying to burn reams of paper, if it happens to be in the communications center. In Teheran, we immediately destroyed all of our classified information and holdings and all of the cryptographic materials in the communications center.

The electronic file storage device is a modified version of the communications equipment we had in place. We use this equipment in other missions, not just high-threat missions, for the day-to-day operation and storage of information. People are training on it and it works. The funding for the program, however, has been drastically reduced. I visited with an individual involved in the program yesterday. We are down from projections for the communications element alone that were running in the neighborhood of $24 million annually, to a level of $5 million dollars. Now the number of electronic storage devices that we can put into high-threat posts is going to be directly related to the funds available. What happens the next time they have mob violence somewhere? People will ask, "Where are the communications managers and why didn't they fix that problem?" So I raise the question again of long-term commitment — not commitment when first you have a crisis situation, when you get more sympathetic hearings, but what happens when things quiet down and you don't have an immediate problem.

Student: It just seems like such a logical program, why are the funds for it being cut back?

Branch: I don't know if there's a single answer for that. But I do know that the costs for care and feeding the systems that were put in place reduced the dollars that were available for initial acquisition. That brings me back to my earlier point. It's one thing to acquire a system and to activate it; it's quite another thing to maintain it. The resources that were made available were based largely on acquisition and activation.

Student: Surely people knew when the systems were acquired that they had to keep them maintained.

Branch: Yes. Actually, in this instance, it's the same appropriation. I'm trying to be as kind as I know how to be, but the Executive Branch did not allow us to go to Congress with a request that I thought accurately reflected the resources necessary over the longer term.

Oettinger: You know, you don't have to be too uncharitable to understand. It happens in private life as well; you buy the house and you forget the upkeep. Universities until maybe 10 or 15 years ago were notorious about accepting capital gifts like buildings, and no one talked about maintenance and operation costs. And it doesn't happen at the level of the folks who request it. It's the front office, whether they're called the Office of Management and Budget or the development office at the university, which says God will provide. When the building's up we'll have another emergency and God will provide or the Congress will provide. Is that so far off?

Branch: I think that accurately reflects the action or inaction of some elements involved in the particular program. I'm not sure it is always the case.

Student: Inconsistency is a problem with defense communications that's been around for many years. A critical message, or what we call a flash message, may take 2 minutes today, 6 minutes tomorrow, and 22 minutes the next day to go to the same place. This seems to be a built-in problem. It's directly proportional, I think, to the amount of activity going on during the crisis. Do you see the same thing in your State Department communications and, if so, what's being done and what do you propose to be done about this?

Branch: We have a similar situation in the State Department to answer a part of your question. On the other hand, to date, it has not been unacceptable. One time a message goes through in seconds, and the next time it requires 6 or 8 minutes. We recently redesigned our system. We put in major new switches in Washington and overseas, and upgraded the trunks and terminals, so we have made it much faster. Today it's not a problem. If you experience expanded volume, along the lines we have, and if you don't keep that system constantly upgraded, it will become a problem.

What do you do about it? In my judgment you simply have got to factor increased volume into your communications planning. You must design and implement systems that permit you to move information in a timely fashion. We have been more successful, I would argue, than Defense in that regard. Not because we have any secret but because we're a smaller organization. We have been able to move things from the validation of the requirement to system activation in a much shorter period. And we have, I think, more accurately projected our growth needs, and the dates when activation is required. So we've done two things. We projected in what I think to be a reasonably accurate way, and we installed and activated systems in a much shorter period of time. When we put these components in place we ended up with a system that was much more responsive than before. Now having said that, it was not always rapid, reliable, and secure. Five years ago our system was reliable, and it was secure, but it was certainly not rapid. It would take us three days to move a routine telegram through the system, and flash telegrams in a stress situation could be delayed in the network. Two or three things happened. First, individuals wanting to move information gave it a fictitious precedence. It became almost impossible to recognize the make-believe "Immediate" from the real "Immediate," and the system started to choke even further.

For the last year and a half, we have run tests repeatedly in different periods. There was a period when we had about three crises running at the same time, each of which involved a number of other posts. That's the other thing to remember. In our world when you have a situation like the Falkland Islands event you have an address pattern that is a lot more than Buenos Aires and Washington. Information was being sent to many of our posts, and much that they sent was being given wide distribution, so you aggravate it with a multiple address pattern. At this time, when we had three crises at the same time, we had somewhere in the area of 1700 immediate telegrams in less than a 24-hour period through the communications center, more than 200 flash telegrams, and absolutely no complaints. But again, how do you deal with system design, anticipated volumes, and projections, and then the big problem — one that most people still haven't sorted out — how do you keep the system updated? That's the same case I'm arguing when I question the wisdom of a separate system to deal with emergencies; how do you keep both systems going?

Student: How serious are people about doing that? Are people really trying to build separate systems, or do more people agree with you that you want to build on top of the system?

Branch: I think most would subscribe to the integration with the day-to-day system. I would at the same time suggest to you that a lot of folks who do studies and make recommendations don't know or don't consider what's in place today.

Student: I've just finished reading *Beyond The Hot Line,** a book by William Ury and Richard Smoke at the Harvard Law School. They would like to see a system jointly staffed by Soviets and Americans in Moscow and in Washington. Now if you try to move your Soviet military attaché into the National Command Center or into the State Department control center, you're going to have some real security headaches.

Branch: You've introduced a host of problems with that concept, in my judgment. You raised the security issue. The next question I would ask is what information is being sent and received? Does it circumvent the normal organization? That gets back to the organizational issues we discussed earlier; your formal structure ought to reflect informal structures. If you have these defense centers, and with all due respect for the Senators, what information flows? Is the defense attaché fully aware of the information flow?

Student: They're not referring to these as defense centers, they're referring to them as nuclear crisis centers combining both the diplomatic and the military functions. Senators Nunn and Warner have jumped on this idea and approached the President in a personal way.

Branch: Yes, I know, and I'm quite aware of what they've written, and I'm quite aware of the responses. I know how difficult it is for this Administration to try to project to the Hill a responsive attitude in terms of trying to do these things, and still deal with the realities of the negotiations. In this paper they talk about the nuclear risk reduction centers in the Soviet and American capitals. The centers would be "linked both through communications channels and organizational relationships to relevant political and military authorities."

Oettinger: Which paper is this?

Branch: I'm now quoting from Jon Boyes' article in *Signal:*

> The group advocated that the direct communications links definitely include print and facsimile channels. Consideration might also be given to the establishiment of voice and perhaps teleconferencing facilities as well. In an earlier study, the Center of International Security and Arms Control, Stanford University, October 1983, advocated a U.S.-U.S.S.R. joint center to support cooperative efforts to prevent accidental nuclear war, and meet the requirements . . .

There's a good deal of discussion in this article on joint centers. I still come back to my point — you can staff centers with diplomatic personnel and military personnel, but have you indeed gone through the existing organizational structure? If you have not, how do you coordinate with it?

I'm reminded of an observation that Dr. Baker made in his role as Chairman of the DTS Policy Board. By the way, I'm probably as impressed with that individual as anyone I've ever met in my life. A young man briefed him on just this issue of reconstituting the government, and Dr. Baker asked what are those lines between those different elements, Defense and State and other elements. The young man said, "Well those are the lines for moving the information back and forth between the elements so we can coordinate in a stress situation." And Dr. Baker's observation was, "Well, you know, in that kind of a stress situation, those centers are going to be pretty busy

**Beyond The Hot Line: Report to the Arms Control and Disarmament Agency* (forthcoming, Spring, 1985).

doing what is theirs to do, defense, diplomatic, intelligence or whatever." The young man persisted that indeed they're there for coordination of activities between those elements, and this was in the most dire kind of a circumstance that one would envision. Finally Dr. Baker said, "Not to press the point, but I want you to know, young man, it won't work; you're going to coordinate this government to a standstill." If you don't use the existing structure, then somewhere after the fact you have to bring your own information back together. If it has come through the organization in the first instance, and it's part of the existing organization, the decision making process, it is less likely that you will have to start coordinating after-the-fact reports. So that's one observation I'd make. I would also remind all of you that notwithstanding what our individual or even official desires might be in terms of these kinds of centers and their usefulness, it takes two to tango.

Student: Are we losing sight of the original purpose of the hot line as we get it confused with confidence-building measures? It is a confidence-building measure, but it's an element of confidence building that goes well beyond that when you look at the war avoidance and war termination function. There's a lot more to it than just the nuclear threat.

Branch: But the hot line really came out of our arms limitation talks; it reflected our foreign policy objectives and our nuclear arms policy. So, if confidence-building measures are indeed measures where we are together trying to find ways to avoid a nuclear incident, then I don't know that we have shifted that much in terms of application.

Student: It just seems there's more of an expanded role for the hot line; that maybe people refuse to or haven't focused as much as we do on other areas.

Branch: It has been installed for 20 years. The government believes it appropriate and timely to examine other applications, and to consider whether or not it would be of further use to us dealing with stress situations. I'm not so certain but that we shouldn't explore joint military command centers, or the nuclear risk reduction centers. Certainly there is a desire on the part of the Administration to find some way to diffuse crises, should they occur. And we're facing a different set of circumstances. We cannot dismiss the possibility of a terrorist nuclear threat. That's certainly different from anything we have faced in the past. The threat is changed, so the application of our resources, in this case the hot line, it seems to me, ought to be examined.

Oettinger: I wonder whether you can pursue that for a moment, because it seems to me the problems about security and such would arise more if you visualize the original purpose as addressing U.S.-Soviet confrontation. But if you visualize the purpose as joint Soviet-U.S. concern over third party intervention, I wonder whether the picture wouldn't be drastically changed in terms of what you need in such a center — what inputs, and what the security problems would be. It seems a somewhat different kind of game.

Branch: You're right, the application certainly has direct bearing on what kind of security problems or challenges are presented as a result of a joint center.

I would leave you with a question we didn't touch on: to what degree should organizations now be restructured reflecting the technology? In the Department of State I was the advocate of change in organizational structure. My thought was that the structure ought to reflect more accurately the technology.

I'll give you an example. The command center in the State Department, our operations center, the one that puts together task forces to deal with crises, is interoperable with other command and crises centers in the Washington area (perhaps not as well as it should be, but it is). We support it from the communications standpoint. At the same time, the telephone system that supports that center belongs to an office called Operations which runs the motor pool, the building maintenance, and the telephone systems. When the General Services Administration managed telephone systems, Operations was responsible for the operation of that system because it was a General Services kind of function. Operations is in the process of replacing the telephone system in the State Department with an automated system that could be an important model in the information flow, and an integral part of moving information between foreign service posts and key principals in the Department; however, the system will remain part of Operations. I'd take issue with that. I know I'm not going to get to restructure organizations sitting here, but I know the Department of State and organizations in general are structured largely around historical kinds of relationships, and I wonder if they shouldn't more accurately reflect the technology and its applications.