INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

Information Technologies and Multinational Corporations
John Grimes

Guest Presentations, Spring 1986
Clarence E. McKnight, Jr.; Robert Conley; Lionel Olmer; Harold Daniels; Mark Lowenthal; Richard J. Levine; John Grimes; Bobby R. Inman

February 1987

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-87-1

Information Technology and Multinational Corporations

John Grimes

Since 1985, Mr. Grimes has been a professional staff member of the National Security Council, where he is Director of National Security Telecommunications and Director of Defense Programs (C^3). In previous assignments, he served as Deputy Manager of the National Communications System, from 1981 to 1984, and as Assistant Deputy Chief of Staff for Operations and Plans, U.S. Army Communications Command, from 1973 to 1981. Earlier, he was Deputy Director, Communications Engineering Directorate, and Chief of the Command and Control Division of the Test and Evaluation Directorate, U.S. Army Communications-Electronics Engineering Installation Agency.

I received a letter some months ago from Dr. Oettinger asking me to explore with you intelligence, command, and control in the business world and the strategic advantages or vulnerabilities that changes in information technology present for multinational corporations. Since my experience has primarily been with the government, and most recently at the national level, I will try to extrapolate this experience to both the public and corporate sectors.

When we talk about information technologies, the term is meant to be all-encompassing — it involves the human element, which is crucial in the decision support role; the hardware and software to store, process, and manipulate information; and the communications transmission and feedback path. Most of you have probably reviewed some of the previous years' proceedings of this seminar series. I draw your attention to the Spring 1984 presentation by a close friend and colleague, Dr. Richard Beal.* He made two points in particular that I wish to underline. One concerned the dynamics of the human element in high-stress situations, focusing on the President and his advisors (which I do not plan to dwell on since Dr. Beal covers it well). The other point, which I'll use as my point of departure, concerned the problem of too few or no tools to synthesize all the information that comes to the decision maker. Information technology can play a major role in performing that function, and today I'm going to discuss the advantages and the vulnerabilities of information technology.

It goes without saying that we're in a fast-changing environment in the information world. The changes are primarily being driven by technology. That's a pretty strong statement, but I think I can make the point. If we look at the deregulation and divestiture of the nation's telephone industry, it was not driven just by the economics of the industry but primarily by technology, which provided opportunities for new companies to introduce more efficient and competitive systems, such as digital transmission systems and enhanced services using such technologies as transistors, microcomputers, satellites, and fiber optics. Entrepreneurs have exploited technology innovation in the marketplace, and it has caused a major change in our capabilities for information communication, retrieval, storage, and processing. Let me give you a couple of examples. In a corporation, it is not unusual now for the chief executive to have

*See Richard S. Beal, "Decision Making, Crisis Management, Information and Technology," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1984*, Program on Information Resources Policy, Harvard University, Cambridge, MA, February 1985, pp. 5-19.

a terminal next to his desk, which gives him direct access to the corporate data bases or allows him to communicate directly through electronic mail to all levels. You may categorize this process as command and control if you wish, but it has a major impact on management's control in the corporation, allowing the CEO in some cases to bypass middle management. Some layers of what we know today as middle management may vanish because of the advent of information technology.

Satellite communications is another of those technologies that permits both the military commands and corporations to "skip echelon," and communicate directly from the corporate head or commander down to a division-level organization. General Motors has installed a pervasive satellite system that will reach down to depot level. In the national sense, we can do the same thing today — go from the White House, or from the Secretary of Defense, right down to the foxhole. Satellite and information technology have made communications flow transparent from top to bottom of an organization. There is an excellent example of this. Back in the mid-1970s, during the *Mayaguez* boat incident in Cambodia, a two-hop satellite transmission path was established over which President Ford was able to talk to the battalion commander under fire on the ground. Here you had the Commander in Chief of a nation talking to a guy right on the ground or, as they say, to the foxhole. This skipped the chain of command from the Chairman of the Joint Chiefs of Staff, the military command in the Pacific area, and the intermediate command in Thailand. Multinational corporations do the same thing today, especially overseas operations.

I want to elaborate on how we use computers and communications satellite technologies for crisis prevention. Information is received quickly from various intelligence and diplomatic sources; it is processed and made to control or prevent a crisis from escalating. Today, I think you would say that in a *controlled crisis*, whether in a corporation or the government, the CEO (or, in our case, the President) is able to be directly involved at all levels of the units involved in that crisis because it's no longer beyond his span of control.

What has computer data base technology done? It goes without saying that technology makes more information readily available through data base operation, but it also is a tool in a decision support framework, which goes back to what Dr. Beal was talking about. You need some kind of assistance in handling all the data input. You must build various thresholds and trigger points into your decision support system. Information is much more timely and accurate today, and data base access is available globally thanks to satellite technology.

One aspect to which many of us give little thought and rarely use, and that I mentioned earlier, is *feedback*. Computer-based communications systems and decision support systems provide an excellent real-time accounting record or result of the sequence of steps that take place during an event, whether in a corporation or the government. Feedback not only helps to complete the record of what transpired, but also drives future policy or changes. In our case, we've learned that when decisions are made in a major crisis and certain actions are taken, standing policy will change.

Computer-based decision support systems, including videotext, video teleconferencing, facsimile, and other visual aids, give more efficient capabilities, and enhance crisis management decision making. Before we had computer-driven display boards, we used to track aircraft by having individuals put radar tracks on Plexiglas boards. Today, those tracks and decisions are made on a real-time basis with computer-based technology. Gaming and modeling of economic situations in a multinational corporate setting illustrate the advantages that technology provides for decision-making tasks.

Real-time video teleconferencing is seeing increased use in the government for day-to-day operations and we're seeing it explode within the private sector. The cost of travel and the fact that people don't want to get on airplanes because of the terrorism threat in themselves increase the demand for this technology. Not only does it improve the use of time but it also lets you see individuals' expressions and gestures during conversations. We're going to see more of this technology used in command and control and even in intelligence operations. The intelligence community can transmit a map or drawing from one country, or one state, by facsimile machine, which is pretty efficient, or can display the material via video teleconferencing, and then record it. I might mention that facsimile technology is used to improve the accuracy and speed of information flow over the Hot Line between the Soviet Union and the United States. Facsimile or video teleconferencing is real. The reason being, getting back to satellites, the efficiency of transmission systems operating on T-1 carriers at 1.544 megabits, versus what we used to run, 2400

baud. Today, we multiplex video teleconferencing, telephone conversations, and data transmission all on the same wideband digital circuit for efficiency and reduced cost.

There is a major *vulnerability* to all of this. We have become so dependent on some of these tools that when we do lose the capability under certain circumstances or for a certain function, it causes chaos. The banking industry is concerned about the financial information that they transfer, to the point where they put error detection and correction capabilities (redundant paths) in their systems so that the information is transmitted in two different ways. In any decision process, from a corporate decision to a national decision, you can soon see that if you don't do some smart things with this technology it can get you in trouble; it's like putting all your eggs in one basket.

Because of these vulnerabilities and demands for ensured connectivity, companies like AT&T have network control centers to maintain the system integrity, and restoral for everything from an earthquake to a regional event, like tornadoes and hurricanes. Other carriers have established so-called operations centers or control centers. Electric power companies are looking at the same thing. They do it primarily for economic reasons, because their profits are based on revenue; when you lose major customers for a long period of time, you lose revenue. Dissatisfied customers tend to switch to a different provider; although the electric power companies in this country still have a monopoly, the telecommunications people do not any more.

As most of you realize, the government does not own a pervasive and independent electric power source or its own telecommunications systems. We get about 95 percent of all our communications from the private sector, i.e., telephone companies. One of the things we've done with both the power industry and the telecommunications industry is to make them aware of the vulnerabilities of their respective industries and encourage them to develop contingency plans and capabilities so that they could restore critical service in case of a major disruption. "Critical service" is defined according to national priorities, depending on what kind of service is being restored and in what situation; the priority may be public safety during a disaster, or service to the Defense Department during a wartime situation.

The electric power grid is now almost totally *computer* controlled over communications links. They have had some brownouts and blackouts due to failures of this technology; while it has improved the overall operating efficiency of the system, it can create tremendous inefficiency when it breaks down. An example — on the West Coast, in the summer, power is shared from the northwestern part of the United States down to the Los Angeles area, to run the air conditioners. In the winter, it is reversed and electric power is shared to the north to run the heaters. The control is done by computers and telemetry flows over communications link.

One other point that I think you should keep in mind is the impact of our changing telecommunications environment on internal corporate management structures. Telephone and computer costs used to be incidental in the operations of an average business. Today, many corporations are integrating those capabilities as a *single information resource* because of technology and it has become a major cost factor. Because it has become a critical and costly element in the operations of a major corporation, the information resource management function has been raised to a vice president level in corporations. The same thing is happening in the government. We now have integrated (for the most part) telecommunications and computer operations into what we call information resource management. Again, that was driven by two reasons. First, technology has integrated the two functions; second, they have become very costly items in the budget, so you want to do smarter things to reduce that cost. I guess I could add a third thing to it: Just as in the case of the power and telecommunications industries, as you put all those eggs into one basket, you also have to do some smart things to provide some redundancy or "backup" for those critical functions in times of an emergency. That imperative applies at all levels, whether it's a national crisis in the case of the federal government, or a local disaster in the case of state or municipal government, or financial risk in the case of a bank, or network integrity in the case of AT&T.

Those are some of my observations on the vulnerabilities and the advantages of information technology on command and control in a macro sense.

Student: You were talking about the survivability of a power system, for example. It seems to me that when you talk about survivability, or increasing the performance of the system you have two rather opposite ways to go about it. You suggested that increasing the integration of a system would allow the slack of one part of the system to take care of the vulnera-

bility of another. Or, decentralizing the system would reduce the likelihood that the failure of a node would produce a system failure. Aren't those two approaches contradictory? In fact, if you continue moving toward greater integration, as you indicated in the case of the power system, then you might possibly tend to decrease the slack or redundancy of the system and make it more vulnerable to general failure.

Grimes: Let me first make a point on survivability. Survivability can be regarded as a matter of life and death or as a matter of improvement by degrees. Take the national power grid system. There's a couple of things that you can do. You have single point failures. One of the things we are finding out is that power plants are not as critical or as vulnerable as substations, which become critical single points. You can do some things today at power plants to take away that vulnerability by using network design. Previously, that kind of solution was not feasible, whether for cost reasons or for regulatory reasons, where the Public Utilities Commissions (PUCs) wouldn't let the companies do that. We have what amounts to a national power grid system.

To come back to your point about integration, the system does become interoperable, but we try to make sure that the loss of one part of it does not take the other part down. We try to take some degradation into account within the integrated system. However, that means that if you do lose a part, you have to have a plan. For example, maybe you're getting power from the Canadians and you lose that as a major source, but you have an alternate plan; in the case of the Northwest, there might be a connection into the Colorado area, for example.

So while parts of what you're saying are correct, I think the systems are so designed in this case as to allow for the danger that you mentioned. We talk about interoperability, rather than integration. A lot of times, integration implies that if you lose one part, it drags another part down. In telecommunications we have some of those kinds of problems, because when you're operating at megabits, synchronization is critical in order to maintain what we call bit integrity. There's a master timing source; somebody always has to be able to clock. We are looking at ways to make sure that the system maintains its integrity because under the new telecommunications industry structure, with so many long-haul carriers — the new MCIs and GTEs, and then the satellites — there has to be one very accurate clocking source, or else you get buffering. It's these kinds of things we have to address to prevent a system failure. In a digital system, if you lose the clock, it's catastrophic; in an analog system it is not. The old frequency division multiplex allowed for slow degradation.

Today, one of the vulnerabilities of a digital system is that it's almost binary: It's either there or it's not. By the way, a very major concern of ours in networks that support national systems is interoperability or alternate routing capability. It used to be that we operated through what we called frequency multiplexing. Today we do time division multiplexing. The difference is that frequency multiplexing worked like your radio; you changed frequency to pass different types of data. Today you code a bit, which is in a serial stream, interwoven with a whole bunch of other information, not even all your own information. When it gets to the other end it's multiplexed out. There's a lot of room today for error and degradation, and you can do things in the system to keep the highest priority systems on the air, whether they're circuits or customers. Today you can lose everything, so you must plan your systems accordingly. That applies to maintaining telemetry on a hardware system as much as to transferring information for a customer.

Student: Is there a general theory that ties together all these concerns about system vulnerabilities and integration?

Grimes: Well, again, the vulnerabilities can be categorized. A corporation that is revenue-based is looking at it for lost revenue, and will go some distance toward ensuring against failures according to the costs and benefits involved. That's an interesting calculation right now with the increase in terrorist activity around the world. Fortunately, we have had little problem in this nation. Some years ago we had a thing called the Monkey Wrench Gang running around out west. They were environmentalists concerned about the big transmission towers that run across the nation, both the metal and the wooden type trestles, the very tall ones. They took blowtorches out there, in the case of the metal ones, and cut them off and just let them hang. It was a very costly proposition. In another case, they took chainsaws and went out where there were telephone pole trestles, and cut those off and let them dangle. They took high-power rifles and shot up transformers and substations. It took quite a bit of time to replace one of those transformers.

Again, that's very localized, and you can do things to get around that loss. If you take a larger event, a tornado or an earthquake in California where you take out a hunk of the system, then you have another type of restoration you've got to consider. In the case of California, for example, communications companies try not to put much cable around the San Francisco area because earth shifts tear the cables. They use a lot of microwave. Also, those shakes "detune" the microwave beam. Companies do various things, like deep piling in the ground, to prevent that. So there are things you can do to guard against some kinds of disruption. But for cases like the Monkey Wrench Gang and terrorism today, physical protection of those facilities has now become a major issue, and corporations are going to have to start doing something about it. Some companies put chain link fences up, with no lights or open gates. Just as you see in Washington with the sandbags, etc., and in airports with the metal detectors, you're going to see that kind of protection as a common practice, unfortunately.

If you carry that one bit further into a wartime situation, we have national policy and plans and organizations in place to handle such things as restoring critical functions or reconstituting the systems. In the case of communications, it's the National Emergency Telecommunications System that works with the 22 federal agencies to set up priorities, so that we can restore those most critical systems that we need. In the case of the power system, the Department of Energy has worked that out and coordinates with the power companies on a daily basis.

Oettinger: I wonder if we could get you to refine a little bit more what I think I heard you say about technology driving things. You did indicate that you were going to concentrate on the technological aspect and not say so much about the people aspect of it; but I'd like to get you to bring people into it a bit more now. Yes, there's a lot of interconnectivity, which you described as creating the possibility of micromanagement. However, the accounts that we had from General Stilwell* and General Cushman** at some of our earlier seminars suggest that, although the connectivity and so on provide the possibility for the boss to get on somebody's back and micromanage, pretty soon people learn how to cut themselves off again. In other words, while the technological possibility is there, with a little care, you can avoid excessive microcontrol from the top. As another example, some people have been complaining that with the possibility of more communications, messages are getting longer. You've heard some of the field commanders complaining about that. Again, that would seem to suggest that yes, the possibility is there and it's being exploited. On the other hand, if you look at the Hot Line, it seems to me that over the years it has been fairly carefully controlled so that there is not excessive or even a great deal of communication.

Depending on which examples you pick, you could make a case that, yes, technology has driven some changes, but only to the extent that people have chosen or allowed them to occur. Sometimes you end up with a purely technology-driven change, but sometimes you end up with almost the exact opposite of the impact technology would have produced, depending on how people want it. So I wonder if you could comment a little bit more on the interaction between what the technical possibility is, and what folks really want to do to modulate, cancel out, or even reverse this technological possibility.

Grimes: When I say "technology-driven," I feel strongly that it's not a pull system out there. We have things coming out of the laboratories that push opportunities out, and then smart people take advantage of those opportunities. The explosion has occurred in the ways people apply that technology to various needs, which in our case is information processing. I think that everything you said to me just now is correct, but for a different reason from what you suggest. Let's take the Moscow Hot Line, a unique system, where technology is providing improvements as in the case of facsimile. The reason the system does not get used is inherent in the uniqueness of the system itself: It's one of the most critical decision points, or warnings, available to us to avert nuclear war. You don't want to use it on a day-to-day basis because the day a message comes in on that, and the bell rings on the Teletype machine or facsimile, it's for real.

Oettinger: But it has a great deal of human discipline; it's not just a case of technology determining things.

*See Richard G. Stilwell, "Structure and Mechanisms for Command and Control," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1985*, Program on Information Resources Policy, Harvard University, Cambridge, MA, February 1986, pp. 33-66.

**See John H. Cushman, "C^{3}I and the Commander: Responsibility and Accountability," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1981*, Program on Information Resources Policy, Harvard University, Cambridge, MA, December 1981, pp. 95-118.

Grimes: But that's because there's a very specific command and control function that it is performing. You have to be very careful about the application of a system. In this case, there's only one Hot Line in the world like this, and it's there for a specific purpose. There's an agreement between two nations that the only thing it's to be used for is an accidental release of a nuclear weapon, although they're talking to the Soviets about expanding it to include nuclear release by a third party, an unauthorized person. The reason why it does not get used is that when it is used, something significant has happened. If you used it every day, as in the Libyan situation last night,* its significance would be diluted. For difficult times, there are other channels that you would normally work, diplomatic channels, which can convey information directly from the White House to the ambassador. When you bypass the embassy and go leadership-to-leadership, there has to be something awfully significant going on. The Hot Line serves precisely that function, but I think that's kind of an isolated case.

Going back to your point about message generation, you made two excellent observations I would like to elaborate on. For one thing, it seems that when you give people more information they want more. Once they learn how to use a system, they continue to get more and more messages regenerated. I know that General McKnight** has been having a terrible problem, because people have adulterated the military system. When they send a message out, they not only send it to the individual addressee, but they also give an information copy to the world, without realizing the burden it puts on the system. A smart staff person knows how to use a system like that, because sometimes the guy actually receiving a message does not have the authority or ability to react as well as one or two of the information addressees. It's a very interesting point to play. Once again, technology gives you that opportunity to use or control information.

I want to go to your first point, on the issue of micromanagement. We're in a transition: Those born since 1960 who've gone through school have had the opportunity to operate a computer terminal, and that becomes a norm in their life. Individuals like myself, and you, Tony, came out of a generation that did not have that opportunity, and there are many people who are scared to use that technology. I happen to have a terminal at my desk that I use for electronic mail, but I still don't get on it and use it for all the other things it can do. It's a very powerful tool. I can tell you my replacement, 10 or 12 years from now, will be more proficient in using that capability; of course, that proficiency also helps to increase the amount of message traffic. Even in the armed forces, we're seeing that the younger kids coming up now who learned to play Atari and all the computer games are doing much better in the military as we introduce these new computer-driven systems, because they know how to use keyboards and their various functions. It's a normal thing for them. It would not be for me to go out there in the battlefield and use those systems.

So I think there's a couple of things in here. I think that technology has provided an opportunity, but we've needed a new generation to exploit it. In the transition we're going through right now, you're seeing the addition of the human aspect, of the people who have to want to seize that opportunity. Anybody born since 1980 will undoubtedly have the same exposure to computer operating systems, or information systems, that we've all had to the ABCs. I think it's a normal thing.

Student: At my agency, we introduced a lot of automated equipment among people who never had that experience. While I agree with everything you said, part of our transition seems to have been an exception. We had to switch people from typewriters to CRTs for transmission of information at a faster pace. They all made it. Some of them were reluctant, but they were able to do it. We ended up having a whole generation who never had any real exposure to terminals suddenly becoming functional with CRTs. They agree with me 100 percent. But when we tried to introduce CRTs at higher managerial levels .....

Grimes: That's what I'm talking about.

Student: ..... we encountered a CRT phobia. I don't know why that is. If we could do it at the analytic, technical level among people who were not proficient before they came to our agency, how come we can't do it at a higher management level?

Grimes: I submit to you, though, that those individ-

*The U.S. bombing raid on Libya, April 14, 1986.

**General Clarence E. McKnight, Director, Joint Command, Control, and Communications Systems (JC^3S). See General McKnight's presentation earlier in this volume.

uals who did learn will use that capability much more as they move up into the organization. My previous boss, Mr. MacFarlane,* was very enthusiastic about using his electronic mail and data bases, and he stayed on it hours a day and late in the evening. My new boss, Admiral Poindexter, is even more so; he has a background in that field. I think our business in the National Security Council has taken on the character of those two individuals with all the automation being introduced. If a different person had been in there, I doubt whether we'd ever have been able to spend the money or move out. As I said earlier, it's a function of the generation that was trained. From here on out, to go back to Tony's point, it will be a question of people knowing how to manipulate the technology. The computer hacker is one example where people get smarter in what you can do with these devices. Similarly, we're going to have people rising into the higher level managements who will make that capability mandatory in an organization. In fact, you read about it all the time.

McLaughlin: Let me add one observation on the generation gap. In the lower levels of the organization, the introduction of the desk-top terminal or access to a mainframe frequently removes the drudgery of the job. I spent years as a budget and financial management analyst, and 70 percent of that job, GS-7 through GS-12, was spreadsheets. There should be, I hope, thousands of disemployed budget analysts in Washington today who used to be spreadsheet artists. All the fun part of that job was when we were not doing spreadsheets. With Lotus 1-2-3 you can now do them in a fraction of the time, allowing you to start actually doing program reviews, interviewing the program staffers and that kind of thing. The higher up you go in the organization, presumably the less drudgery there is associated with the job. There is less stuff that you can throw off on the computer and, therefore, perhaps less incentive for the 50- or 55-year-old manager who doesn't know how to type and was not trained on the computer to move it onto his desk.

Grimes: I think a lot of it depends on the type of organization, the product, or the service. In recent years I've read some books, right out of this school, indicating cases where upper management goes in and gets reports on production, product lines, delivery times, etc., and just bypasses all of the middle management. The question is how to control that process of blending technology with management. Well, again, as individuals become more proficient and comfortable with it, I think it's going to become more pervasive in time. You will find that it will change organizational management schemes for those companies that use it.

Student: I'm not sure, because I think there may be a natural reluctance to micromanage through technology; rather than interfering that way, someone might prefer to let people run their own management as they were trained to do years ago. In other words, one may choose to follow a set of management principles based on the idea of letting subordinates "do their own thing," letting them be entrepreneurs. Another principle of good management says that you're supposed to be walking around out there just visiting, not micromanaging; you're just supposed to be getting a feel for what's going on. Even though electronic mail and other capabilities allow you to micromanage, you might not want to do so. On both counts, technology may be running up against current management principles that discourage taking much advantage of that technology.

Grimes: I don't know. All I'm saying to you is that you're at that point right now where management and technology have run together. It may be that in some places the CEO or the executive vice president for marketing and the younger managers will make more use of that phenomenon, while older middle management resists. But it's already happened; that's evident from some of the research going on.

I kind of tie that to Tony's point about controlling the amount of information flow. In the military, young officers all understand how to use information flow so as to be more effective, to get things done by going to different points. That ability is increasing. A guy like General McKnight, who is from the old school, has to deal with the effects of this new capability; it's breaking down the chain of command in the military very quickly, skipping echelon and changing who releases messages. It used to be that only the commanding officer or the adjutant general could sign out a message. All that technological capability, in the name of proficiency and accuracy, is playing havoc with the command structure. It goes back to my point earlier about communicating from the White House to the foxhole. During the Vietnam War, President Johnson supposedly spent every night

*Robert C. MacFarlane, former Assistant to the President for National Security Affairs.

in the "Situation Room" deciding what sorties went out and what targeting to choose. He could do that because of excellent communications back and forth to Vietnam. We all understand the speed of light; it didn't take very long for that information to come in. That is micromanagement at the highest level.

Again, you can do some of that as long as it's in a controlled situation, in the sense of the span of control that is possible; you could never operate an entire war that way. One of the concerns that commanders expressed when I attended the Army War College was that, as you gravitated over a period of time toward skipping echelon, getting away from the commander's prerogatives, you might end up in a major change where you turned over a region to a commander and he had to make decisions that he was not sufficiently prepared to make. This is not something that happens overnight; it's an evolutionary process. That's where I see technology driving changes in organizational structures and procedures.

McLaughlin: That process may be self-correcting in a sense. After the Ford White House got burned in the *Mayaguez* incident, they didn't want to have it happen that way again. The chain of command was very carefully partitioned in the Korean tree-cutting incident, and that line didn't go to the President. That flavor came from both ends. The White House didn't want to play the same game and, of course, General Stilwell and General Cushman didn't want to play the same game. I think you've gotten to a point in this administration where the White House has been willing to say, "That's a military matter where we won't wake the President." That may cycle back again. Right now I think it's very clear that military stuff is done militarily, perhaps to a fault.

Grimes: It takes on the character of the guy at the helm, though. You've got to remember that. If you want to talk about a *Mayaguez*, I don't think this President would ever do that. He believes in corporate or macromanagement, and leaving war to the experts. He'll make the decision that we're going to take a hill, but not how we're going to take it. Another individual, as we've seen, might assert himself in deciding how we're going to do it. Technology has given you the opportunity to do that. Whatever information is available at the White House today to make those decisions is pretty much just as readily available to the other agencies, only we see more of it. The same goes for corporate headquarters, whether in a domestic company or a multinational corporation. That kind of information is available because you design that data flow into your system so you have some finger on the pulse. You can start seeing if things go awry.

That brings back the point of whether it's a push system or a pull system. People can very subtly cause thresholds to be built. If something happens at the General Motors plant in Spain that exceeds some threshold, you throw the first warning signal back to corporate headquarters. The same goes for the national level; there's some threshold as to whether you're going to wake up the President at night.

Student: You've painted a picture of great quantities of information flow and quicker feedback. How does this affect resource requirements? Does it indicate more decision support tools for a President Johnson, or more resources for analysis? Or are the two related and developing in consonance?

Grimes: It depends on the context.

Student: You gave the example of decision makers having to make decisions quicker now because, as happened last night, the media get the information much faster and put pressure on the decision makers. So what does this mean for the other part of your capability, your analysis capability?

Grimes: Sometimes it's harmful because you have to make a decision, and so you go with the information you have and make an analysis based on that. The analogy with a corporation may not be exact here — for a corporate decision the deadline could be in days, whereas if you're talking about national security or national welfare, it's got to be in a matter of minutes or hours. I don't care to speculate on the minutes. If you have a conventional situation or a crisis situation like last night, you get some kind of an analysis or assessment of the reaction. Those reactions can come from a number of sources, whether it's the public, or the news media, as in our case last night, or other intelligence sources. You accumulate a pretty quick feedback. If you were in a critical wartime situation, you may not even wait for that information to be analyzed before making your assessment because you're already developing a strategy on your next move; that's the element of surprise. But in a crisis like last night's Libya raid, a one-time event, you'll make an immediate analysis. Then you also try to determine the intentions of, in this case, your adversary, and in the case of a corporate multinational, your competitor. Again, it's a matter of degree. You can develop all kinds of sce-

narios. But you have to be very careful not to generalize too much.

Student: Is there a danger that, because of technology, the information flow is getting faster while there's always a tendency for analysis, being less measurable, to slip behind?

Grimes: That risk is definitely there. One of the ways you might overcome it is to improve the decision support capabilities to take in that information, and artificial intelligence is going to help to improve that process. What we're talking about right now is almost on the same threshold as the Strategic Defense Initiative (SDI). When you're trying to respond on a real-time basis, based on your warning, your sensors, there's no human mind that can react fast enough. That's where artificial intelligence will start doing a lot of that recognition for you and giving you options very quickly. Again, you have to play out the various scenarios, whether you're talking about a nuclear conflict versus a national crisis such as last night.

You can take the Bhopal disaster with Union Carbide as an example of a very major crisis, looking at how they set up emergency operations, collected real-time information, and weighed the decisions they were going to make, including the possibility that the Chairman of the Board might have been locked up and held hostage when he arrived. It depends on the circumstances. In a military situation the primary concern is the element of surprise. The risk is that the information flow is so great and so fast that sometimes the analyst has to go by intuition.

General Stilwell is probably one of the last old-timers around. I happen to know about the tree-cutting incident a little bit. In fact, I went to Korea after that to see how we could improve communications to him, when he was the commander out there, so he could have real-time information. Maybe he didn't want the President to have it, but he wanted it himself. He didn't let the commander on the scene handle the situation. Just between you and me, he wanted to know if we could hook up the new night vision devices out at the posts along the DMZ to a transmission system and send information to his headquarters in Seoul, in Yongsan. He's a pretty senior guy and has held some prominent positions. But in essence, he was just going from his command down to that guy on the post. So if an incident started, he could sit in his little command center in Yongsan and watch the events unfold. What was he going to do? He was going to be like Ford, or Johnson; he was going to be making decisions in place of the commander.

Oettinger: It's fascinating to compare that account with Stilwell's, because you seem to corroborate what's emerging as an important principle of information systems design: Cut me off from my boss, and keep me in the fullest possible contact with my subordinates. Everybody at every level seems to want that, quite independent of technology. Although there was a bit of surprise when the technology snuck up on people, they very quickly relearned this principle in its contemporary version and started taking steps to apply it. You also seem to have enunciated or hinted at another emerging principle, in connection with the Hot Line. In that unique and extreme case, since there are few things quite as important and crucial as avoiding nuclear holocaust through error, you're saying that a strong incentive exists for disciplining and limiting the amount of communications, so that there is no babble that might hide genuinely critical information. Whereas more relaxed or routine applications are producing the effects that you described General McKnight as having to deal with. So the principle seems to be that where things are critical enough, information explosion is not a problem because you control the amount.

As you reflect on your experience, do you see any universals or principles or patterns of information use where technology may create a momentary blip, but then the needs reassert themselves?

Grimes: When I worked for the Army Communications Command, as more and more computers were being introduced into the system, initially for logistics or what we call support functions, we tried to discipline the system. But because of the large amount of information in the division and the corps, commanders all the way down to the battalion level became so dependent on their computers that if they were to lose those in a stressed environment, they would have no other continuing operating capability. In other words, they had nobody trained as what we call a "stubby pencil." When you requisition units in Europe or Korea, it's a pull system. It's not an environment where some historical forces are pushing the requisition system, such as when you know the failure rate of airplanes and certain types of tires that you've introduced and you can automatically program the system to send fuel or tires at intervals based on usage and so forth.

My point is that with this increased proliferation of computers in every aspect, in the medical area, logistics, transportation, etc., our dependence on them is causing a major strain on our communications capabilities, especially in the tactical environment. When you're operating in a benign environment, your pipe is very large. When there's a disruption in that pipe and you've got to go down to half the size, setting priorities for what is the essential data you need becomes very critical. Unfortunately, people think that they're going to operate in a stressed environment with the same amount of information as they have in peacetime.

The Moscow Hot Line operates in a very controlled environment limited to two individuals, and was designed to pass very critical information on an accident or an error made by either party. Its purpose was not for going to war, but for preventing war. Whereas with these very pervasive systems scattered in 16 divisions or air wings around the world, so much information is flowing out there to sustain that force that the systems now in use during peacetime are going to cause problems when you get into a stressed environment and have to disturb the network.

Oettinger: Let me see if I can get you to speculate a little bit as to what the remedy might be. If I go back in history, it seems to me that it is precisely for that reason, among others, that the notion of doctrine evolved in the military: What do you do if the horse and dispatch rider don't get there? There are certain things that you do when you get cut off. To some extent, what you're describing implies having lost sight of some elementary principles. If so, then maybe a correction should be on its way. Or have we not yet had enough experience in stressing these systems, with the pipelines breaking down, for people to have relearned and reinvented doctrine or modes of operating when they're cut off from the pipe?

Grimes: That's a very interesting point. I don't think that we've had enough major impacts yet, something catastrophic where individuals have been fired or lost their jobs, to have forced us to try to discipline those systems that General McKnight talks about all the time. I just don't think it's happened. I think you could use Vietnam as a benchmark; that was the first time that we made heavy use of communications systems, both military and commercial, and they were never disrupted because we were operating in a controlled environment. We are concerned about going into an environment where someone intentionally disturbs or disrupts your communications. To take a commercial example, you may have been following the Home Box Office (HBO) encryption problem, and how people have gotten very excited because they're being denied free TV. I can tell you that one of the reactions has been to interfere with the HBO signal, which denies a large customer base its TV, which in turn means a revenue problem if it's done enough, as people then change to a different service. There are efforts in Congress right now to look at the problem; people are also taking covert measures on their own.

To go back to the point you were making, I think we're now recognizing the need for doctrine and procedures to deal with stress environments and communications disruptions. The two technologies of computers and telecommunications have merged now to the point where that need has arisen. It used to be that the computer people did not coordinate with the communications people; they just took it for granted that the communications source would always be there. But we got in such dilemmas in the Army and elsewhere that those functions have been merged, because it was recognized that neither one could go without the other in today's distribution systems. I think it's a self-correcting problem. We're seeing some efforts now, and progress is just a matter of time. We just have to hope we're not faced with a life-or-death situation before we get there. That's kind of the critical point. We do have a propensity for uprighting; we swing one way or the other, and somehow over a period of time, our checks and balances kind of set us straight.

McLaughlin: It seems to me that part of the problem is the continual need to reinvent common sense. Your logistics pipeline is not going to be there either if someone's attacking it. That's why you carry certain stores and ammunition with you, on the assumption that you're not going to get resupplied on a daily basis or whatever in certain situations. That logic is basic to contingency planning in general. But it seems as if every time we put in a new technology out there with new opportunities for communicating, we keep forgetting that we won't have all that pipeline available and that we have to plan accordingly.

Grimes: Tony used the word "doctrine." Doctrine of course is used more in the military than in other federal agencies or in corporations. Doctrines, goals,

and objectives are somewhat similar in a sense, but doctrine means, "This is what we're going to do and how we're going to get there." In most government organizations I've been associated with, as computers became available, people never went out and used the computer as a more proficient tool to improve the process. They simply automated the existing one, two, three, four, five steps involved in a travel voucher or transportation form. Now, I think it's generally understood that with all the edit functions and accuracies of computers, you can do away with steps two through 10, because the computer does all that for you. Ten or 12 years ago, I pushed very hard to have the office of the Army Adjutant General at Fort Benjamin Harrison start looking at what office automation computers would do, because they put out all the procedures and regulations on general, common user forms, personnel records, and so forth. If you automate that recordkeeping then you eliminate a whole lot of functions; when you do that efficiently you also reduce the amount of data that you have to process or transfer. That's starting from the very beginning: You lay out what you want to do and you take an analyst in there and say, "This is how you do it," and then you write your code around it. That kind of process is starting to police itself. Again, you've got more people who understand computers and their applications, whereas previously there was always just a handful of experts around.

McLaughlin: The pattern you described has been very common in industry. It has been our contention for some time that if you went out and did a methods study preliminary to buying a computer, you would wind up saving all the same money without buying the computer at all; the computer simply provides the icing on the cake. The general pattern is that people tend to start by automating what they've already been doing, and then only later do they rethink the actual process once it's automated.

Grimes: Another point that we haven't talked about yet is the trend toward establishing corporate communications centers. It has been brought about by the structural change of the telecommunications industry in this country. As most of you know, about 80 percent of the network out there is owned by AT&T today. Of the rest of it, about 10 percent is MCI, and another eight or nine percent of it, maybe not quite that much, is GTE and U.S. Telecom, while the rest is strewn about. The concept of end-to-end communications changed with deregulation, whether for a computer, a telephone, or any other information system. Corporations have had to change the way they do business. Companies like General Motors and American Airlines have all had to go out now and develop a corporate infrastructure in order to maintain end-to-end communications for the various information systems they use in their day-to-day operations. Cost was one important reason, as I mentioned to you earlier. It used to be that you went to one vendor, AT&T; you told him that you wanted to go from A to B, whether or not you knew anything about 2400 baud or 4800 baud, and AT&T would provide that service and just send you a bill. Because of increased costs and rapid change in regulations in the competitive marketplace, people are now out there shopping around for cheaper service.

The result is that corporations not only have added a vice president for these functions, but they've also had to go down and put in what we call control centers, staffed with smart people who know how to order that service. In some cases, they have gone out and built their own systems, or are buying dedicated systems, because it's much cheaper to do that. But if you do that and you want to maintain end-to-end connectivity, you've got to have an infrastructure in order to restore service during an outage. Again, that means you have to build yourself a little control center with competent people in there. You've got to be able to isolate the problem, whether it's the computer or whatever. You're seeing a major trend in the environment for that reason. That's a part of information systems.

A prime example of what happened in government is the case of the Federal Aviation Administration (FAA) at Oklahoma City. Oklahoma City is probably one of the largest nodes for communications for our federal government for administrative purposes, and the FAA was only getting service from a couple of major carriers. When they were required to go out on a competitive basis and get service from other carriers, and had to operate with the local exchange carrier and install their own modems on the ends of the circuits, they got into some real difficulties to the point that they had to build a control center and staff it with five people 24 hours a day. It's costing us taxpayers a pretty good bundle to maintain that reliability that we wanted from end-to-end service. In the case of the FAA, even though it's an administrative center, it involves some critical things that have to be done overnight, like sending spare parts to radios in a Los Angeles airport. Also, it's the library,

if you will, where accident information is deposited and those kinds of things.

The point is that deregulation has driven our whole culture. Where we used to rely strictly on the telephone industry to provide all that maintenance of end-to-end service, now we're getting services from various vendors — the local carrier, the inner city carrier, and then the suppliers for the devices on the end. It's costing you dollars to coordinate all that. Deregulation has created a marketplace for a new service, network management; corporations either hire individuals to work within the organization, or contract out (in the case of the government you have to work directly for them). A General Motors or an American Airlines is big enough to have its own management people. But now there are companies, GTE and some smaller ones, that are in the business of managing your information resources. That's an interesting situation that has developed over the last three or four years.

McLaughlin: As a follow-on to that, how well do you believe the federal government has done in acquiring the resources to manage its own systems, instead of bringing in AT&T for all this?

Grimes: Most of the federal agencies that made heavy use of the Bell System have had to grow that capability, such as the Federal Emergency Management Agency (FEMA), the Department of Energy, and the FAA; the Department of Defense has always had military controllers, but they've had to be trained to take on this extra duty. I think that after three years, we have now pretty well developed that capability within the government, but at a cost.

Oettinger: You've been talking about the cost to the taxpayer for these control centers, network management services, etc. Are you aware of any studies or do you have any impressions as to whether or not, in compensation for that cost, you've gotten more reliability? This goes back to some of your other points about redundancy, etc. The Bell System made a point of having alternate routing and so on, but one could imagine that a decentralized network with these little control centers here and there could be more robust. It could also be more chaotic. Or it could all just be an illusion; everything might rely on the commercial control centers underneath, as a system is no better than the underlying network. From where you now sit and have sat, are you able to form any judgment as to whether we've had a net gain or loss in robustness?

Grimes: If you had asked me that question a year ago, I'd have said we had a net loss, but we've grown in that area of expertise and we've put into place some functions to overcome that difficulty in the government. I'd say all things are about equal now with where we were three years ago. I'm talking primarily about the critical command and control type of information systems. Today the federal government gets about 90 to 95 percent of all its communications from the private sector. As I mentioned, AT&T probably owns about 80 percent of that 95 percent. Anyhow, because of that dependency in the federal government on the private sector for what we call national security and emergency preparedness (NS/EP) circuits and services, we have had to establish a capability in Washington such that, in the event that we did have a national emergency, rather than turning to one vendor for end-to-end service, we would have a national coordinating center in Washington to overcome that deficiency that grew out of deregulation. Although the government paid for the facilities, the 12 major carriers of this country have individuals posted there at no cost to the government, to ensure that service is continued or restored, or that a new high-priority service gets installed. That center does not coordinate the total telecommunications service for the government, only the most critical, and that's a very small percentage.

I haven't seen anything to indicate that we have better or worse service today than three years ago, other than that there's a lot of confusion in people's minds outside of those who deal with telecommunications on a daily basis and understand that relationship between the two technologies of computers and communications. I can't refer to any studies. I will add one other aspect to that: Under the National Security Telecommunications Advisory Committee (NSTAC), we're looking at the network to see where we can do some smart things to restore service between corporations. But, again, that's only for national security; that's not just for anybody's use. Yes, we have done some things to make the system more dynamic, and yes, decentralization may give you some improvement in robustness because it gives you other alternatives. I don't know of anybody who has done any study, or analysis, or measurement of that improvement or degradation.

Oettinger: But your sense is that, after a dip, at least within the government, the critical NS/EP capability has come back to roughly where it's been?

Grimes: Yes, I think it has.

Oettinger: If you project that, would it lead to an improvement over where it was or remain status quo?

Grimes: I think it's at its plateau now. Of course, we've been trying to influence the rest of the world — the nations where PTTs* continue to dominate the telecommunications market. We're seeing change in Japan and the UK.

A lot of other interesting things have emerged from deregulation and divestiture. For example, it used to be that when we had a visiting dignitary, a head of state, AT&T had the wherewithal teams to furnish service wherever that individual traveled in the country. We've had to change that. We've had to put in our own capability to accommodate those individuals because AT&T is no longer the sole provider of communications. When we had the economic summit down at Williamsburg, AT&T kind of coordinated that for all the telecommunications companies. Now that function is being left up to a government entity.

The other side of that change is also of interest to you: The diplomatic corps itself is asking how we ensure that, under certain conditions, we maintain communications to their respective posts or embassies here. We've had to set up a mechanism within the State Department, the Office of Communications, so that if they've got a difficulty in getting service or need a new kind of service, we consider that need as a matter of national security and handle it accordingly. So a lot of side issues have come out of this.

McLaughlin: You referred earlier to Richard Beal's remarks of two years ago on the lack of modern technology when he arrived at the White House in 1981, and the efforts at the NSC to introduce modern facilities. He talked in particular about installing new video conferencing and facsimile facilities to link the White House with key centers. You've mentioned teleconferencing, but has there been much progress in video conferencing since then?

Grimes: Sure. I guess I must have dropped the word video. I thought I had put facsimile and video teleconferencing kind of together. It's a good point, and you're right. At the time that Richard was talking about, the best TV you had was regular wideband, using the normal TV bandwidth which is not readily available. Subsequently, there have been some major breakthroughs in coding techniques and compression techniques for 1.544 megabits. For command and control at least, it's now very adequate and, of course, the cost has come down and the service is readily available. It is being used now almost like the telephone service you order. In fact, approximately two weeks ago, I was at the ribbon-cutting ceremony for the Army Materiel Command, which had just put in a video conferencing network between their nine major commands. It operates in color, again at 1.544 megabits, and it's working well. Only when you have some fast movement do you get a little bit of tear on the screen, and that's because of coding.

To show you how fast it's moving, Charlie Wick, the head of the U.S. Information Agency (USIA), has put in a thing called World Net that he's operating around the world now. He sets up a conference with some of our leaders in this country, and perhaps some local politicians or local news media, and that's done in real-time video conferencing. The State Department has done a survey on video conferencing for certain posts and is looking at that. For some posts the value would not justify the cost. Industry is already out there. The American Satellite Corporation and some others are installing private systems that are used on almost a full-time basis now between organizations or major corporations. The technology's here. It's like computers or anything else. It's taking time for people to get used to it. As I indicated, though, I think you're going to see a major increase in the use of video conferencing, not only because it will cut down travel costs per person but also because I think terrorism will keep people off airplanes.

Some people at the senior level of government will not get on a video conference, especially in a stressed environment, because people can see your stress gestures, sweating and so on, when you're worried about something. It also goes back to the question of individual choice in applying new technology like that. But it's been introduced, it's being used, and it's moving fast. The system that Dr. Beal was talking about was a standard TV channel, which is very broad and very expensive. Since then, we've been putting out new systems over satellite. It's very easy to set up, because you can take a mobile satellite terminal, on 1.544, and set up a video conferencing capability right here in a matter of probably an hour,

*Post, Telephone and Telegraph: foreign government-owned telecommunications monopolies.

if you wanted to do it between two points at the narrow beam. The fidelity of it, as people might call it, is not the same as TV, but it's close enough for most events.

McLaughlin: It makes me wonder about the interaction of deregulatory actions. I heard a J.C. Penney representative last week talking about the fact that they were using a lot of video conferencing (which made me feel it might finally be real after all these years). One of his observations was that executives had found it harder and harder to travel in the post-deregulation milieu and, therefore, were more willing to participate in video conferencing. They had many locations that used to be a day away by plane, but aren't now.

Grimes: As I said earlier, computers are now just another medium for information flow, and the convergence between computers and communications will change structures. It used to be that, if corporate headquarters were in New York, you might have to go out to the West Coast once a month, whereas now, every morning at eight o'clock you might hold your staff meeting with those guys in it. You've already started to micromanage that guy on the West Coast, if that's your nature. Don't get me wrong; it's just that the opportunity is there. Video conferencing is another one of those technology-driven innovations that I call opportunities. It's there and it's going to change the traditional way of doing things over a period of time as it's introduced, and as a generation comes along that is used to it.

In high schools now they teach public speaking in front of a camera. You get used to that. When I was at this ribbon-cutting, general officers were still shy of getting on video conferencing to talk, because they were concerned about their appearance, and so forth. But it's one of those things that I guarantee will be common by the end of the century. In fact, the technology is such that the old AT&T picture phone that they ran from New York to Pittsburgh on a wideband channel will not be an uncommon thing in your home by the end of the century, because of progress in compression techniques. You can't do a lot of fast movement, but compression techniques and coding techniques are such now that you can almost transmit that on what we call ordinary telephone line, at 9.2 kilobits.

Student: Is there any teleconferencing going on in the corporate world where it's not between two individuals or a small group of individuals, but where a chief executive like Lee Iacocca gets on a telephone that is hooked up to auditoriums all over the country in all of the corporate organizations? Could he could pick up a phone in a studio with the camera on him, and talk to 6,000 people who are part of Chrysler Corporation?

Grimes: Yes, that's going on. The 6,000 people may be congregated in 10 places. In fact, during national party conventions held each year now in hotels around the country, they bring the local delegates in and hold the business sessions on suppressed TV. They're doing a lot of that.

McLaughlin: Every major Holiday Inn, for example, provides that service. If you want to have your regional sales meeting out here in Dedham at the Holiday Inn, they provide the dish and zap the meeting room so that the president of the corporation can come in and talk.

Grimes: That's an excellent example; Holiday Inn has put in their own telephone service that they run themselves. You can call long distance over their services between two points, off net. If you stay on their facilities, they will readily provide video conferencing so that you can put on as many people as you like, 600 people in 10 places. That's not uncommon. At the Army Materiel Command, the four-star commander has two studios in his headquarters, and he can go out to his nine two-stars on video conferencing. It's unbelievable how efficiently it's operating. It's a voice-actuated AT&T system. The Army is expecting to cut down on travel with it. Of course, it's secured with crypto devices and the studios are also secured; that's a very crucial point for the military.

Oettinger: Historically, travel and communications have grown together and I remain skeptical as to whether anything profound enough has happened to reverse that.

Grimes: I agree; but the Army's goal is to offset the cost of this system by saving on travel. I happen to share your viewpoint, because at Fort Huachuca, Arizona, we've put in a network and conferencing capability and it didn't cut down that requirement. People just like to travel and get away from the job, to clear their minds.

Student: In our agency, the chief visits all the stations once a year, but what if he has too many stations to visit within a year?

Oettinger: True; or suppose you're vulnerable at too many airports or one thing or another. And yet, 10 years ago the argument was that the rising cost of oil would so increase transportation costs throughout the economy that for energy conservation purposes, why, we would have a takeoff of conferencing, etc., etc. Now the argument is that maybe it will be terrorism or difficulty of traveling or something that will do it. The historical evidence remains that there is a very robust correlation between transportation and communication, and that one seems to feed the other rather than replace it. I don't know. It seems in some respects counter-intuitive — one might think, "Gee, if I can talk to 6,000 people without moving, it ought to save a whopping amount on the transportation bill," and some day that may even be true. What I'm saying is that historical evidence today shows quite the contrary.

Grimes: I have to make one other point. It rather surprises me that nobody's raised it yet. I gave you some of the advantages of information technology, and then I discussed some of the vulnerabilities. I talked about dependency on the systems, and the possibility of losing the service; but I'm really looking for the $64,000 question, one that Congress is concerned about: Big Brother.

Let me just elaborate on it. As technology does all these things for you, probably the most controversial issue that we as a society have before us is the security, or privacy, of this information and its exploitation by individuals with unauthorized access to it. I don't know where that's going to go. Of course, we're in a free society, and we're very conscious about limiting controls — it comes back a little bit to what I just told you about HBO "free space," where the attitude is, you get what you can. One of the major vulnerabilities of information technology is that when you transmit information, whether it's military or corporate or personal information, someone can get access to it.

While the government has had to address this issue for many years, and has done things to protect information — particularly critical military information — industry has not yet accepted interception as a threat to corporate planning, other than those companies that are in high technology arenas. Some of the high tech firms have been required by law, or by contract, to protect certain information. Access to computer data bases and systems has become a major issue. Unauthorized access by the Soviets to high technology data bases in the universities, through various associations and exchanges, etc., will probably be the most highly debated information issue over the next five years. Technology can fix the problem, I think, to a point. You can't entirely stop it, we know that; but in the main we can fix it. Yet, when you apply certain secure techniques, then you deny other people access to that information, whether for economic or technical reasons. It's going to be a major debate in Congress and in the Executive; General Stilwell is involved with it, and also Congressman Ed Brooks (D-TX, Chairman, Government Operations Committee). It will pose a constitutional question eventually.

Student: There were two news items in regard to that this week. One is that NSA's offer of endorsement to industry's standardization of cryptographic equipment for the private sector makes it more secure to have industrial communications, but some also say it makes information in society more available to NSA. The other item is that DOD supposedly wants to go into disinformation on weapons or contract information in a big way, putting spurious data into the system so as to confuse potential information gatherers. Actually, those techniques, to deny an enemy information and to overload him with false data, seem to come at the problem from two different ends. Considering the nature of American society, overload might be the more promising of the two, but difficult to carry out, I suppose.

Grimes: Well, the government has made no actual claim of disinformation, even though accusations to that effect have been made in the media. I can tell you, from where I sit, that there has been no conscious decision or policy to do that. I can't say the thought doesn't reside in people's minds. Actually, I think we're already engaging in overload because anybody trying to sort out the information we publish has a major task ahead of him. But if somebody wants to spook the system, to get at corporate planning, stock market information, or bank records, they can; you've got to look at the various threats. There are hackers out there who have been put into jail, and are back now as consultants to industry and to individuals. Security is a real issue in information systems. All I'm saying, as a closing remark, is that it will be the major debate in government; we can fix most of it with technology, but I'm not sure we want to do that because we might end up denying information to people who do need it. It's a national issue that we have before us, and it won't be resolved in an hour's discussion.