INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

National Security and the Democratization of Information
David Y. McManis

Guest Presentations, Spring 1989
Stuart E. Johnson; John F. Magee; John T. Myers; Charles A. Zraket; James M. Fox; David Y. McManis; Robert T. Herres

August 1990

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-90-3

National Security and the "Democratization" of Information

David Y. McManis

David McManis is the Director, Operations Security Organization, of the National Security Agency (NSA). He has been with the NSA since 1960 and has held a wide variety of analytic and management positions both at the Agency and within the national security community. He has been Chief of Staff for the Information Security Organization; Director of Foreign Relations in the Directorate of Plans and Policy; Chief of the National SIGINT Operations Center; Chief, Office of Support to Military Operations; Executive and Chief of Staff, Telecommunications and Computer Services Directorate; and Chief of Information Resources Management. He has spent much of his career supporting various elements of both the executive and legislative branches of government, including five and one-half years as a member of the Senior Staff, National Security Council, and Director of the White House Situation Room. He completed two years on the National Intelligence Council as National Intelligence Officer for Warning and Director of the National Warning Staff under William Casey. Mr. McManis has made oral and written presentations on warning and information handling to universities, military commands, civilian departments, and foreign intelligence establishments.

Oettinger: I asked our speaker today to lead the discussion on his democratization of information theme, or whatever else is on his mind. He'll do, I'm sure, something like that. I will not burden you with his biography; you have had a chance to read it, so you know all about his background. I just wanted to add to it the good news and bad news. The good news is that he is one of my oldest friends and it's a real pleasure to welcome him back here. The bad news is that he knows me too well and, as a consequence, has requested that the first 30 minutes or so of his presentation be uninterrupted. So, with that, the next 30 minutes will be uninterrupted Dave McManis. Dave, it's all yours.

McManis: I don't normally do a formal presentation or written presentation but Tony and I have talked over a number of years now. The interest I've had in information as a resource has grown and grown, and when I talked to Tony about coming up here, I decided that there was so much that I wanted to try to say, that there was no way I could do it just extemporaneously. So I wanted to have a relatively short, formal presentation and I hope it will in and of itself generate lots of discussion. Then it's really fair game, and I don't even mind, if I outrage you too much during the formal presentation, if you want to throw rocks. I can probably handle that as well.

What we have been looking at over the last few minutes is a videotape which was made in the Numerical Laboratory of Dr. Karl-Heinz Winkler at the Los Alamos National Laboratories. We've been looking at the modeling of certain hydrodynamic events using algorithms compiled for supercomputer processing. Now the data rate from the image device to the display screen is 60 million bits per second. In this case, each of these several-minute segments that we've been seeing comprises as much as 5 to 10 million bits of data per second and each took approximately 120 minutes of Cray XM-P four-CPU time.

These are numbers that I can't begin to fathom. I just know they're damn big. That kind of power just totally blows me away. Tony also caught onto the fact that this goes back to my roots as an art-history major and I really enjoy these presentations for their intrinsic beauty, but I think equally impressive is the complexity of their development.

The point I really want you to think about is the incredible ability of your visual and cognitive systems to absorb so much data in such a very short time, precisely because of this graphical representation. Our human eye-brain system has an ability to handle over a billion bits per second, so we're not really taxing our physiological capabilities, but most significantly, it's our ability not just to accommodate these tremendous data-transfer rates, but also to readily identify the patterns, disturbances, and anomalies. This visual interaction with the supercomputer has been identified by Dr. Ken Neves of Boeing Computer Services as one of the tremendous information breakthroughs of the next decade. I want you to keep this in mind as we progress through my presentation today because I'm frequently going to refer to our inability to cope with data being collected and presented to us. But I do believe that the technology can provide us with better answers if we could ask some better questions.

With this high tech preamble, let me go to the subject of the presentation, which is the "democratization" of information and its relationship to our national security. This also gives me a chance to show some travel slides.

Let's talk about what I mean by the democratization of information. Over the past decade, the western world has been evolving at an ever-increasing rate. Virtually every part of our society has been touched in some fashion. In industry this ranges from everyday bookkeeping functions, through inventory control, automated design of microelectronics and macro components, and even automated assembly using advanced robotics with both visual and tactile capabilities. Slide rules for engineers are passé, and as I learned from my engineering grad student daughter; they have been replaced with inexpensive calculators which not only can be programmed, but which can also represent mathematical and statistical calculations graphically. Your own personal physician most likely has automated the administrative functions in his office, and may also be very dependent on automated medical databases for complicated diagnoses and to identify the latest treatments for specific medical conditions. Even the public libraries, the last bastions of hard-copy information, are now becoming information resource centers with automated, on-line access to commercial databases which contain literally billions of bits of information.

Certainly the evolution of the computer, in terms of relative cost performance trade-offs, has been the key factor in the explosion of this technology. But at least as important is the revolution in telecommunications which has enabled the massive linking of computers and databases through communications networks. Stand-alone, isolated computers are today's Edsel. The true information power of the computer can only be realized through networking with other processors and databases. As you've heard time and time again in this forum, not too many years ago Tony coined the word "compunications" and he's never been able to live that down. But that did certainly recognize, perhaps for the first time, the symbiosis of the two technologies. Not only can the user today have direct access to enormous databases at reasonable cost, but also in many cases access to the latest supercomputer processing capabilities. University supercomputer consortia are allowing more engineers and scientists to develop and model complicated processes in relatively short periods of time that only a few years ago might have taken years, if not lifetimes.

The security of the country is also critically dependent on the evolution of information technology. Never has our national leadership had such timely access to such a variety of information, nor such impressive ability to process, manipulate, and display that information. When I was at the White House in the late 1960s and early 1970s, we were highly dependent on narrow bandwidth information channels and most of the information received was in the form of semiprocessed or raw information. Our first automated communications upgrade used a processor with less power than that found on most desktops today. In contrast, the President today has more capability to get data when he travels than we used to be able to provide him at home. Richard Beal, with whom I worked at the White House in the early 1980s, noted to this forum that, "We spend billions and billions of dollars to collect information, to get it from the field to the analyst in the bowels of the bureaucracy, but we spend virtually nothing on direct support to the senior policy maker."*

*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.

Unfortunately, despite some physical improvements in the information handling at the White House, our true ability to support the decision maker has not improved commensurate with the technology. In some ways we have only confused the decision process with enormous increases in the rate of data exchange.

Information in the western world today has become a valuable commodity which is appreciated, utilized, sold, traded, and stolen, and impacts every facet of our daily lives. This is the democratization of information to which I refer. Eastern democratic societies, such as those of Japan and Korea, are also beginning to recognize the importance of the information resource. But for the time being they appear to be focusing primarily on the tools necessary to manipulate the data, not on the information itself.

With this evolution has also come a dependency on the information technology which makes it imperative that the decision maker retain timely access to these information resources throughout periods of stress and crisis. As in the civil sector, automation and networking have brought about miracles, but have also created significant vulnerabilities. During my career in the national security community, which has kept me heavily involved in command and control and the supporting information handling technologies, I've observed a fascinating evolution. I've been impressed by the rapid changes in technology and frustrated at the slowness of our application of that technology to improving the information resource. As is often the case, this evolution has occurred either very rapidly or very slowly, depending on your point of view. Looking back over my career of 30 years, I can honestly say that I'm amazed by how far we have come, although there are still many challenges known and yet to be discovered.

I started as a young analyst before "real-time" was known. As the primary government analyst on several international crises, I knew that even cartographic data was limited. The *New York Times* or the *London Times* served as our primary alerting source, and even that information was days late. The good news, at that period of time, was perhaps that the decision maker had a much greater time frame in which to operate.

Since the beginning of the history of modern warfare, command and control has been viewed as the critical ingredient. It wasn't until the development of modern electronic communications and communications networks in the 1960s that we discovered the critical importance of communications. Modern forces were being deployed around the world, as a tool and asset of U.S. foreign policy. However, contrary to the procedure in earlier times, the National Command Authority modulated the activities of the force on a continuing basis, and this heightened the requirement for a global connectivity with our national leadership. Additionally, modern military tactics made it essential that the battlefield commander have good and reliable communications with his subordinate units. President Johnson, during the Tonkin Gulf incident, discovered the importance to him of the direct connectivity with the tactical force commander, and thus a new era began and communications changed "command and control" to C^3 — command, control, and communications.

As C^2 grew to C^3, battlefield commanders began to accept the importance of intelligence. The intelligence community, as a result of the same communications technologies that were supporting command and control, was now able to provide timely information about enemy strengths, force deployments, and occasionally intentions to the commander, and thus effectively multiply his force capabilities. Intelligence support, now that it was of tactical utility, was recognized as the fourth key to successful battlefield and crisis management. In the early 1970s, "C^3I" emerged as the watchword. Many have claimed credit for coining the acronym, but the truth, which only Tony and I realize, is that I was the one who coined the term. Nevertheless, the important fact is the recognition that it is the synergy among the four factors that provides us with our strongest possible defensive and offensive capabilities.

The telecommunications explosion which has served to strengthen the United States and our national security has also yielded a potential vulnerability, in that the adversary now has many more opportunities to access our most sensitive information and operations and take his own countermeasures for preemptive actions. The U.S. government last year acquired an estimated half million PCs and the figure is expected to double this year. Thus, the challenge of securing our information resource, and protecting our vital secrets, is becoming increasingly more difficult and tedious. We must be concerned by the various threats being presented to our compunications systems which have been most vividly exemplified by the recent and well-publicized examples of computer hackers.

In 1986, an astronomer at Lawrence Berkeley Laboratories detected the repeated attempts at computer penetration by an unidentified outsider. Rather than taking steps to deny access immediately, Cliff Stoll began a lengthy investigation into the intruder's acti-

vities, which eventually led to the arrest of the intruder by West German authorities late last year. Over a ten-month period the intruder had attacked about 450 computers and successfully entered more than 30. Just within the past few months, West German authorities have allegedly connected the intruder with the KGB, and now they think the intruder is probably more than one person. In this instance there was no successful access to sensitive data, but the incident served public notice that our information resources are very vulnerable to attack and that attack can serve to access our most sensitive data, corrupt our data, destroy our data, or deny us access to our processing capabilities.*

A number of issues are raised by this enormous vulnerability of our communications and computer systems. The first of these is the privacy of our data. The fourth amendment to the Constitution guarantees to every citizen the right to privacy, which extends to their personal data and intellectual properties. Furthermore, it is the right of the individual to identify which information should be protected. Despite this, without additional safeguards, personal data from individual medical files, financial records, etc., can be accessed or manipulated by unauthorized persons or organizations. Credit card fraud alone, which results from the unauthorized access to account numbers, accounts for from three to five billion dollars lost annually. Full realization of the threat of access could result in a state of anarchy which would make Orwell's *1984* appear tame by comparison. In another dimension, even our friend Opus in the *Bloom County* comic strip has been critically concerned by this privacy issue and the impact of commercial satellite imaging.

Manipulation of data can be equally destructive. There have been instances of manipulation of bank transactions to allow the transfer of seemingly small sums of money to the accounts of unauthorized recipients. Even more dramatic have been the numerous recent cases where large sums, hundreds of thousands of dollars, have been shifted from one account to another electronically and illegally. This is usually, however, the result of insider action or at least the possession of insider information.

There are even more subtle threats that we may need to be on the lookout for. Computer logic bombs or time bombs can have a destructive force well beyond that expected from their relative simplicity. One example, perhaps apocryphal, cites the case of a programmer working for a western power and light company. A simple modification to his company's processing programs was made so that should his name not appear on the company's pay records, the electric distribution grid would be brought down. Sure enough, he was fired, his name didn't appear on the pay manifest, and a segment of the western power grid was disabled until the problem could be found.

These examples are largely in the public arena, but there are equally grave implications for our national security. In the examples I noted earlier of computer hackers, I showed how easy it is at least to approach sensitive, classified databases and processing capabilities. However, there have been no instances of outside access to the actual databases themselves, although services have often been disrupted by real or imagined threats. The application of cryptographic security to communications and databases containing classified information is extremely effective as long as that information remains in electronic form. Compromise, however, most frequently occurs because of unwitting disclosure of related information and activities. We cannot afford to ignore the insider threats against which adequate, technical countermeasures are just now being developed.

Denial of service can also occur as a result of explicit or implicit threat to the computer and communication systems. One recent case of denial of service to national security systems resulted from a rumor that certain advanced processors had a computer time bomb set to go off at a specific time. Consequently, all of the processors were taken down until all programs could be checked and verified as being legitimate. The effect was the same as if the time bomb had been real. No amount of traditional security protection could have precluded that denial of service.

In spite of the problems noted above, all are capable of detection and solution. They are within our power to moderate or eradicate. Systems can be encrypted, audit trails can be established, random passwords can be instituted and changed aperiodically, access can be controlled, and penetrations can be detected.

But the most serious vulnerability, in my view, is not the threat to our information systems, but our inability today to absorb and correlate the vast quantities of information available to the national security analysts and decision makers. Five years ago in this forum I alluded to the problem of too much data and too little information. Despite the technological advances, the problem remains with us today. Our analysis and research continue to be largely automated

*Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday, 1989.

manual processes. Our few forays into the world of artificial intelligence, particularly expert systems, have yielded minimum payoff. We still don't know how to process data and present it to the analyst in a manner that will allow him truly to take the pulse of the health of the world. We are continuing to build enormously sophisticated and expensive collection systems while remaining unable to cope with what we are currently collecting or what is available from open sources.

As a personal aside, I've always marveled at our tendency to ascribe more importance to that data which is the most expensive to collect. In my 30 years, I've not personally been convinced that that is a premise which can be supported with fact.

At the same time, our dependence on the technology is growing and this, in and of itself as I've said, is creating an enormous vulnerability. We constantly risk data overload in our command centers, our weapon control centers, the cockpits of our military and commercial aircraft, and even the offices of our decision makers. Could we attribute the shooting down of the commercial airliner in the Persian Gulf two years ago to the problem of sensor or sensory overload? I don't really know. But it's not unheard of in our combat information centers today to have multiple streams of asynchronous data confusing the decision makers. Add to that the stress and excitement of a hostile event, and you have serious consequences.

Richard Beal and other speakers here have talked about the tyranny of the in-box in the workings of the executive decision maker. This remains an area which desperately needs attention.

I've talked about the good and bad effects of the democratization of information in the West, but what about the impact of the information revolution in the rest of the world? In the Soviet Union the technology gap is proving to have very serious implications for the Soviet economy and is at least one of the causes of the new policies of *glasnost* and *perestroika*. Computational power is lagging that of the West by a decade and the gap is growing. Despite the existence of an "academic computer network," the communications of the Soviet Union remain primitive. There is no significant computer industry that is not built on reverse engineering and the products are notoriously unreliable.

There is another strain on the system which results from new access to information. Oswald Ganley, in one of his most recent papers, points out the following: "During the 1980s, the penetration of Western information through the Iron Curtain has increased substantially. Both in the case of the Korean airliner downing by the Soviets, the KAL 007 incident, and the Solidarity era in Poland, considerable access to Western news and other information was made available to the people of the Communist countries. This access has had a major effect on Soviet and Eastern European foreign policy, causing the Soviet Union, especially, to be more forthcoming. Cross-border television pickup and an increasing number of available VCRs have also helped erode Communist government control over information."*

Perestroika, on the other hand, is a recognition of the economic implications of the information age. New policies have dictated a doubling of the telephone system, introduction of computers at all levels of the economy, and teaching of computer literacy in the schools. Despite the goal of accomplishing this in the early 1990s, it remains problematical whether or not this can occur.

One of the most serious implications of this failure of the Soviet Union to remain technologically competitive is that the strategic imbalance places enormous stress on the Soviet government and could have an enormous destabilizing effect. At one time, we in the United States were critically concerned about a strategic arms imbalance. Today we can be no less concerned about a knowledge imbalance. On the other hand, the Soviets recognize the value of information and are leaders in exploiting open source databases from publications and computer databases. We, of course, do everything possible to make this easy and profitable for them to do.

Another aside, and Tony's familiar with this one too, I've been promoting McManis's SDI for a number of years. One of the most destructive forces to the Marxist-Leninist way of life since Hitler's invasion of Russia could easily be the ready availability of personal computers to the Soviet populace.

In the PRC (People's Republic of China) some of the same problems exist but with a pragmatic twist, typical of the thousands of years of Chinese cultural consistency. The PRC today is economically more backward than the USSR. However, Deng Xiaou Ping has identified the criticality of science and technology to economic reform and the country is beginning to move out. In some ways, its backwardness is making the technological jump easier, in that there is not an existing communications network, for instance, which can be built upon. The PRC is thus trying to leapfrog into the 20th century. In communi-

*Ganley, Oswald H. and Gladys D. Ganley, *To Inform or Control?* Second Edition. Norwood, NJ: Ablex, 1989, pp. 188-189.

cations they are moving directly to glass fiber for their long-haul communications. That will give them the ability to catapult into the information age and give their Asian neighbors and the Soviet Union, and perhaps even the West, an economic run for our money in the long run. They're also emphasizing the need for education in the technical skills and are sending an increasing number of graduate students to the United States to study engineering and computer science. Most important, while there is a potential for a brain drain from the PRC, as is often true of a number of other foreign countries, the Chinese students are returning home. Additionally, there are as many as 20 million excess workers in the PRC, which can be of enormous economic utility if they can be productively emphasized. Finally, the PRC appears to be willing to recognize the need for some level of capitalistic endeavor.

Japan has been under the magnifying glass for some time. They are today a major economic competitor. They are now leaders in applying technological innovations to products for the market place. However, a number of stresses are finding their way into their society and culture. Engineers are finding that they did not choose the proper course to maximum financial success. As in this country, sales is often the best course to senior management positions. Another significant challenge to the Japanese economy is the move of manufacturing off shore to other countries with lower standards of living.

More important, I have not seen Japan as an information society, aside from their ability to make the critical tools. In particular, my dealings with the military command and control systems have led me to conclude that the military is still in the command and control business and has not evolved into C^3I except as necessary for interoperability with U.S. forces.

A brief comment on the Third World, primarily to refer again to Ozzie's book, *Global Political Fallout: The VCR's First Decade*. The Third World comprises everybody else whom we have not previously discussed. To a large extent, these countries remain relatively underdeveloped and particularly their communications and data technology is not developing at a significant rate. However, what we are seeing is the influx of television and the VCR, which has contained significant messages about the United States and perhaps will serve to influence international policies to a degree not yet imagined. The thought that the perception of the United States may be based on a fanatical attention to *Dallas*, *Dynasty*, *Charlie's Angels*, and *Miami Vice* boggles the mind. Ganley notes that, "Video cassettes have also been used to perpetrate specific political acts such as spreading propaganda, supporting rebel guerrilla activities, airing the views of and assisting terrorists, sending messages across borders where individuals are unwelcome, avoiding governmental news blackouts, passing off lobbying as news, and spreading anti-Semitism. They have been used for political purposes by governments as well as individuals."*

I've talked about where we've come from in information handling technology and its impact on national security, and where I see the world today. A few words about the future. I've said several times that I remain very concerned about our collective inability to deal with or cope with the volumes of data available to us today. The efforts of Karl-Heinz Winkler and others to use the full power of the computer to reduce data to manipulatable and understandable images presents great problems. As researchers and analysts, we may soon have the tools which will not only help us cope, but will also strengthen our efforts by improving our understanding of natural as well as political phenomena.

In the area of computer and communications security, the ongoing efforts to change the development of software from an art form to an engineering discipline will eventually allow the development of information systems in which we can place our full trust and confidence.

Neural research may lead us to new breakthroughs in speed of processing and also allow us to move confidently away from digital or, at least, binary processing. Our capability to have a machine help us with our understanding of phenomena and particularly to draw relationships and inferences from disparate events will be substantially improved.

Chaos theory, while allowing us to increase our capabilities to model phenomena, is also calling into dispute the validity of our current modeling networks. One interesting example, which has nothing to do with what I'm talking about, concerns the use of fractals for modeling. It's the comparison between the map in an atlas, where you look at the coastline of the United States, you would measure it as approximately 3,000 to 4,000 miles long. If you went to perhaps a navigational chart, that same coastline would measure about 10,000 miles long. If you were a hiker walking along that same coastline, you would probably have to walk 15,000 to 18,000 miles. And then our friend the ant, who has to crawl over every grain of sand, would clearly have to travel 30,000

*Ganley, Gladys D. and Oswald H. Ganley, *Global Political Fallout: The VCR's First Decade*. Norwood, NJ: Ablex, 1987, p. ix.

miles or more. Fractals have shown us a way of modeling the smallest possible number of significantly large events.

Supercomputing is rapidly being reduced to a secondary consideration in information processing. In 1970, when Tony and I first met, we were developing an automated information processing system for the White House. The power of the mainframe computer, which took several rooms to install, was far less than that which many of us have in our desktop PCs in our offices and homes. Yesterday's Cray will soon be tomorrow's PC.

Finally, during the last administration we reintroduced a technology which has been in and out of favor over the decades: astrology.

In summary, the democratization of information is significantly improving our national security, but we cannot afford to be oblivious to the risks and vulnerabilities. Because of the great disparity between West and East, there will be significant strains for the foreseeable future. Additionally, the dependence on our information resources and the vulnerabilities of those informational resources remain significant. This trend will continue. New technologies are emerging. The linkage between supercomputing and graphics that I started the presentation with is very exciting, particularly to someone like me who has spent so much of his life in the indications and warning business. Adaptive neural networks and neural processing, which will further improve our capabilities to perform pattern recognition and inferencing, also hold significant promise. And now chaos, which is calling into question our capabilities to model phenomena beyond the short term, offers the promise of new modes of data analysis.

In conclusion, I urge you, through your involvement in the command and control community and in the decision-making process, to focus on the information resource and its vital importance to our national security and world peace.

Oettinger: I'm still on my good behavior. Will someone start it off?

Student: I'd like to start with a question that I mentioned to you earlier. When we looked over the recorded annals of this seminar, perhaps the most lively discussion that ever took place was between you and Dave over the idea of surprise in the intelligence system and whether it was possible to ensure against that. As I recall, at that time you took a view that Professor Oettinger characterized as extreme, that we could, in theory at least if not practice, eliminate the possibility of our C^3 system being surprised. I have two parts to the question. One is, has anything happened in the last five years to change either of your positions? Secondly, with this vast amount of information that you're talking about and the confusion of the decision makers, does that also cause you to have thought about the ability for us to be hoodwinked?

McManis: As Tony knows, I pretty much remain an optimist in this field despite concerns that I have. Three or four incarnations ago when I was here talking as a warning officer, I had reasonable confidence in our ability to guard against surprise. I guess I still have that today. In fact, I think the warning processes are good and are relatively healthy. Our ability to collect the kinds of information and to interpret and understand and, more importantly, to convey warning to the decision makers continues to need help.

On the other side of that, a few experiences over the past four years I've been involved in have still kept my feet on the ground because I've seen us continuing to regress to problems I thought we had disposed of in the early stages at the national level. One of my significant concerns has been the difficulty that we as analysts in the community have in doing alternative analysis, taking into account possible scenarios other than those which sort of logically jump out at you. When I was the National Intelligence Officer with Bill Casey, I was very high on Casey because of his not just willingness, but desire, to look at the alternatives to what the common wisdom was, and I think that strengthened our ability in the government considerably. A lot of that was lost. He was a one-man band, or a two-man band with me beating the drum. Some of that is coming back but we're having to teach people the same lessons. We've been fortunate that we haven't had the opportunities for surprise.

There may be another very positive thing on the other side. I think our principal and common adversaries are much more knowledgeable and much more understanding than they used to be. So, by and large, I remain fairly optimistic. Perhaps I had gone off on a cloud of euphoria when Tony and I got into that debate, but the debate was useful because it certainly caught everyone's attention over the years in this course. Do you want to rebut that, Tony?

Oettinger: No, no. I think it's something of a glass half full, a glass half empty. I think David and I don't disagree over the observations, but more over the interpretation and emphasis. I think David is a more devout rationalist than I am. I consider myself a minimal rationalist, believing that on the average it is usually better to know a little bit more than a little

bit less. I think David believes it's more often true and more achievable.

The other part where we don't disagree is that it's a measures and countermeasures thing. I think he admits that where there is increasing sophistication on one side, there are also increasing advantages and disadvantages that are temporary and ultimately you're sort of back where the next level of technological advance is an ephemeral thing. There's a dynamic problem (and this is where that may or may not be a fundamental difference) where, technology and temporary advantages and disadvantages aside, Clausewitz's observations about the fog of war remain kind of fundamental. I believe that, and he may believe that the fog can be dispelled. In the short run, of course, that's often true, but in the long run I guess I'm somewhat less optimistic in terms of making a fundamental difference. I might just go back to your opening with the show of the Winkler tape. I think it has to do with the fact that complexity throughout the history of all mankind keeps growing and then gets made simpler by the kind of thing that you showed which compresses 60 million bits per second's worth of something or other which is unfathomable and incomprehensible into a comprehensible picture which, once again, becomes less complex. So we have these periods of explosion in complexity which then get wrapped up again in a package that becomes manipulable. Depending on what phase of that process you're looking at, I think you can have a greater or lesser faith in the knowability of things, so that's my response to the question.

McManis: Tony was looking back four or five or six years ago. I don't think that our ability to handle data, the process, was nearly as good then as it is today. I don't think we're close to where we need to be in this regard, although I do think the technology is there, but since the 1970s we've had that tremendously short time window in which we had to operate, certainly from the strategic warning standpoint. I should say, though, in the areas of local or regional conflicts or terrorism, at the moment it's an information problem but there's not necessarily much information out there to be gleaned. There still is the capability for surprise if your plane is bombed or blown up, that's a tremendous surprise, although generically we know that's going to happen somewhere, sometime. I remain very optimistic from the strategic standpoint in terms of the major competitors and certainly less optimistic than I was on the regional, nontraditional kinds of problems.

Student: One of the things you mentioned at the beginning is that you spend relatively little on direct support to the decision maker or policy maker, while there's a lot of energy put into the first stages. What are your ideas on what changes should be made?

McManis: I figure we need some very basic institutional changes. Richard Beal talked a great deal about this. I think we still have today decision makers who literally are reacting to the in box and the in box doesn't necessarily have the most critical matters. It just happens to be what got through the system and it may even be too late to respond by that point in time. Having lived for a long time in the White House and having continued to deal with them over the years, I just see this tremendous pressure of trivia that gets put up there. Then the other thing I see which is the fault of the top is the continuing attempt to respond to the *New York Times* and the *Washington Post*, to try to get ahead of them in the decision-making process. But that really doesn't allow for the longer term kind of thinking that we need to have, particularly during times of stress. So we're very weak in that regard. From our intelligence community's standpoint, as good as we are and with as much money as we spend, we still have not come up with adequate ways of distilling critical information and providing it to someone so that they can have confidence in it and understanding of it, but it can be a measurable quantity and a quantity with which they can cope. Again, the technologies have some promise, but I'm not sure I'll see it in my lifetime as a civil servant. We are getting better.

Oettinger: There's an optimistic millenarian streak. I just got a letter yesterday from Michael Zak, who was one of the students in the seminar in its first or second year, and he was reviewing one of our products, in fact Frank Snyder's compendium on command and control. He's been in industry all these years since he left the university and his comment was, with regard to his experience in business, that about the only leverage he thought that a CEO, a president or whatever, had in a large organization or could have, was in the allocation of resources. Nearly anything else resulted in fatal overload or meddling and the implication of what he says is that he's got to be reactive. He allocates resources, and then he sees what his in basket produces, whereas I think what you're suggesting is that he not be that passive in dipping down and looking at it.

McManis: The distinction between the presidency and the CEO is significant. First of all, I don't think the President has much capability to allocate the

resources; he has very little capability, and that's probably a weakness. On the other hand, the CEO doesn't have the capability to push the button and go to war. So we have to figure out what is it our President is supposed to do, and what we should be helping and supporting him to do. We all avoid thinking about the unthinkable; we don't like to think about how you go to war.

Oettinger: So you're focusing on the President as Commander in Chief.

McManis: Yes. The other thing we need to work on is government efficiency. We don't have a bottom line of making a buck, and that's too bad. You should have to make a buck somewhere down the line. There should be something that drives for efficiency other than occasional good management.

Ernst: I'm not sure I can express this very coherently, but it seems to me that we're really dealing with the problem that the presidency in peacetime and the presidency in wartime, for very good reasons, have always had to be quite different. I think that this country, on the whole, very deliberately has not wanted a highly efficient, or even a highly effective government. It has not wanted a President who could do very much in any form of allocation during peacetime. The result is, I think, the whole operational process changes totally in wartime, but in the past we had a nice, big difference that took the law a lot of time between peace and war. The problems that I think you're talking about are how do we take a presidency that, if we want to stay a democracy, in a sense almost has to be kept limited, inefficient, ineffective, and allow it also to be able to handle a very short-term, fast-emerging crisis for which in the past we only prepared by going through a long process of changing all the precedences by which the presidency operates as we go into a war. I think that's the essence of the problem you're talking about.

McManis: Well, you're right in terms of the transition from peace to war and also that during periods of stress, such as the 1960s and 1970s when we had a major crisis every six months, that tended to make the information process much more efficient, but that took time. Today we have less time to deal with it. It really was nice when we had two weeks to make a decision about whether we go to war or not.

Ernst: I think you're right about there being a crisis, but I don't think there's an acceptable solution by saying you ought to make the presidency operate more during peace the way we allow it to operate during war.

McManis: I don't think that's the core of the point I was trying to make. I would like to see the President better supported in terms of his ability to understand a situation, whether it's a domestic crisis or an international crisis. There's a considerable amount that we can do, because if he is well served in that regard then when he is forced to make some very quick decisions, hopefully, he will make some well-based decisions and that's the tricky part we have to deal with. We don't want a totally in-control government, one with incredible efficiency, although I, like any citizen, would like more efficiency than we have today. I think it's a good point — the issue of transition is important.

Student: May I continue with that? In business we say that technology for informal decision support systems or executive support systems for CEOs only have really been able to be implemented successfully when the CEO or the top manager is a person who believes in that. Do you think we have to wait for a new generation of politicians who are the ones who have to finally use these things? Can that be useful?

McManis: Yes, but we're much closer than that. I mean, we're starting to see this new generation get into areas of power. And, again, I think there probably will be some more sophistication in terms of the tools, too. Most of us in this room are reasonably familiar with working with a PC and working a word processing system, if nothing else, some much more so than others. And a number of people I deal with are at very senior levels. We're starting to do that more and more, but even if we had the mechanisms in place, even if we had Sun terminals on every decision maker's desk and we were able to get information from all sources into them, we still don't know what to do with that information. We don't know how to display it — particularly national security kinds of things. How do you display increasing tension in 12 different parts of the world and put it in the proper synchronism so you understand this is happening faster than that is happening over here? It's because we haven't focused on the information. No doubt, the tools are there if we can describe what it is that we want them to do for us. I couldn't have said that even four years ago, but today I think we can say that. Everybody's focusing on building the next communications satellite, the next collection satellite, because there are billions of bucks involved. We need to focus on how you really identify

national security information or create a national security decision system.

Oettinger: We might come back to that. I just alerted one of our students to my desire to foment the discussion between you and him. Let me set the stage. You made several comments in your formal remarks about the threats to the computer communications systems and various hacker assaults, and, therefore, some desire to protect databases and so on against intrusion. One of our students is writing a paper in which he raises some questions about (I don't want to put words in his mouth) U.S. paranoia on this matter and the possible effort, therefore, to shut off access to and export of data to the detriment of other nations, trading partners, or whatever, with specific reference to Japan. Have I explained your concern correctly and if so, is this two sides of the same coin, am I raising a question where there is no question, or what? Can I get you guys to dispose of this or to discuss it?

Student: So far, the United States has the largest databases in the world, and Japan has imported the databases through DIALOG or other database companies. Of course, the U.S. government has been irritated because of the small portion of the databases available from Japan. The United States wants Japan to supply more Japanese databases.

McManis: That's a huge issue; that's a whole seminar's worth of issue. There are a number of dimensions. It's really critical — this is me speaking, I guess, not in any sort of official capacity — for the scientific community to be able to share data worldwide. There will always be economic strains which will cause us to protect our data, but then again, it seems to me that every time we protect our own information, even from ourselves, we end up losing more than we gain. On the other hand, that does not mean that there should not be and that there are not some very sensitive databases which have to be protected from outside users. I don't particularly want people monkeying around with my medical records, although I'll tell you I just got a very good physical, so I'm in good shape. But we've got to find a balance and sometimes we, in the U.S. government, have come off as being fairly heavy handed because we have looked as if we're trying to wrap our arms around all databases and protect all information from everybody. That's clearly not what we are trying to do. We're trying to provide tools for that hard core national security thing which we should keep secret, but also to help Joe Citizen to protect his own medical data and make sure he has some right to privacy.

In terms of a trade-off between the United States and Japan on databases, I guess I've never actually heard that discussed anywhere as being a problem. Certainly in other areas, in market areas we talk about, if you open up more markets for cars, we'll allow more of yours in and those kind of things. I've never thought of those as terribly productive discussions either. I think openness in information to the extent we can do it is a very critical factor, and I think it tends to be a stabilizing factor rather than a destabilizing one. So if there is paranoia on your part, it's probably no worse than on our part, but paranoia is good only up to a point. We need to keep a check on it. I don't know if that's a good enough answer. I don't have a U.S. government policy statement on this thing.

Oettinger: I didn't expect that.

Student: A question on that. What evidence is there to support that certain specific U.S. databases are already being fenced off, that is, are no longer penetrable legally by Japan? What is the evidence that you see?

Student: For example, there's access to DIALOG databases. People living in the United States who have a contract with DIALOG can access those databases. However, people living in Japan, even if they have a contract with DIALOG, can't access some of those databases. Maybe these are science databases.

Oettinger: Why are you taking that so seriously? Because clearly all that means is the necessity to have a Los Angeles office which has the subscription and that's that.

Student: Such a policy is not effective. Why did such a move take place?

McManis: There is a paranoia on our side because, indeed, we became aware of Soviets accessing these databases some years ago through European connections, and we discovered that if you go through some of those databases you can put together a fairly convincing story on how to build an F-16 or something. There's a lot of data that is unclassified but when you put it all together it becomes very sensitive. The answer really is that data shouldn't be there if it's going to be sensitive, but I think we did take steps to cut off direct outside access.

Student: I guess my question in follow-up to that is, so they have an office in LA, I mean, what did you accomplish?

Oettinger: That's the point. We all agree.

Ernst: You've accomplished one thing, and that is that whoever received the information is subject to

U.S. legal actions that might not apply if it was received over in Japan. In other words, presumably, if the Los Angeles office has to draw the data out, if you for one reason had protected that specially in terms of license arrangements, conditions for use, you have got the legal mechanism to enforce it there. You don't if it's gone somewhere else, maybe.

Oettinger: It's all theory anyway.

McManis: The answer is the information shouldn't be there in the first place if it's that sensitive.

Ernst: It might just be commercially sensitive.

McManis: The commercial folks are worse than the government about putting sensitive information out. I'm less worried about them.

Student: I was just thinking about a database that I subscribe to. It's fairly new, I guess about two years old. The U.S. Naval Institute has a wonderful thing called the Military Database. Are you familiar with it?

McManis: No, I'm not.

Student: It's on world armaments; it's just unbelievable as an open database.

McManis: Is that where Tom Clancy got all his information?

Student: From looking at the subscription agreement on the specific method of accessing that, I would see no impediment to anyone anywhere in the world dialing into that thing. That's why I have trouble figuring out what the issue is.

McManis: The government made an abortive attempt to set up this new classification called "unclassified but sensitive," which was terribly misinterpreted as to its intent. But it showed the government's frustration with somehow not being able to put its own arms around the sensitive aspects of government information. In a bigger perspective, it's small peanuts and we've got every librarian in the world upset with us, but I don't think we'll ever try that again.

Student: The Kennedy School bulletin board had a list of databases available in the Washington area, and there was a big list of about 25 of them. They were all free; you could access them from Japan, from Spain, from anywhere, and when you get in them you can get into the Air Force, you have their budget with all the different programs they have, and I imagine we will never provide that in Spain to anybody. Why should you provide it? Would Japan provide that? In trade and in diplomacy you are always acting reciprocally. I don't know why there is so much concern about the paranoia about something that we are not offering. If we are not receiving it, why, is Japan giving that information freely about her budget, about all the air force projects? I wouldn't be so concerned. It's just you Americans. You are really giving more information than we are ever going to give you.

Oettinger: Maybe it's all misleading.

Ernst: We overwhelm you with data.

Student: That's democratization of information.

Oettinger: Which gets us back, I think, to what is one of your central themes, that it keeps growing, whatever it is, and keeps outpacing the digestive or absorptive capacity and so on. Yet your opening example, Dave, flatly contradicts that. Now is your message that in certain realms of science, like fluid dynamics, there is an advanced capability for taking massive amounts of data and putting them in digestible, intelligible form, but that's lacking in, let's say, the realm of the President as Commander in Chief?

McManis: I think it's exactly that. When the President has a display in his office which somehow conveys that much data about the health of the world, then we will be getting close to some significant breakthroughs in handling information. When I, as an information researcher, can pull together some information in some way that will explain to me differently so I'm reacting to a different set of stimuli other than just strings of words I have to work myself through, then we'll have made some big breakthroughs. I know I don't understand how to do that now, much less to explain it. I've been trying to explain to you for 10 years now, Tony, and still don't do a very good job of it. But somehow I know there's something out there. That's the first time I've seen the thing.

Oettinger: Let me try to spell that out because that's one area where David and I have rather common ground. We seem to be either ahead or behind the rest of the world. It is this notion, perhaps somewhat utopian, but that is where my optimism is as high as David's although on a question of applications I might differ somewhat. The development of computers, telecommunications, and so on, is making methods of communication (in a broad sense of getting ideas out of one person's head and into another person's head) available that transcend anything that we have known in the history of mankind by virtue of opening up a pictorial channel which is much more useful and much more subtle, and has much higher capacity, than the eyes, and the ears, and the voice, and so on. The ability to do economi-

cally the kind of thing that was illustrated by that videotape suggests that we are close, and the fact that the capacity may be moving onto people's desktops at an affordable price, may, in fact, be opening up a completely new era in modalities of human communication. Now, who can say what that means in terms of anything to do with command and control or literacy or anything else.

McManis: It's there. But what is it? You know my favorite subject, the indications and warning process. I know that it's a large leap, but somehow it's there. I still haven't quite figured out how we make that leap.

Student: You're talking somewhat about going from number crunching to idea crunching?

McManis: Yes. When this crazy term "artificial intelligence" came out five or six years ago, that's when everybody said that was going to happen. We were going to get big inferencing engines which were really going to deal with concepts and ideas. We ended up with one not very subtle thing called "expert systems" which quickly ran up against the practical barriers. Then robotics, which is a marvelous field but has not all that much to do with information processing. We still have to grab for the next gold ring.

Student: I have a question that is not so much technical but more human. How do you handle authenticity and responsibility in this data? You were talking about data coming up to the decision makers and my experience in the hierarchy is when the decision maker looks at a paper that comes to him, he first looks at the signature. When the person submitting it is known to him as reliable and responsible, then he would take the substance of the message. How can this relationship and this assessment be handled in this technical way of information and this huge amount of information, especially when parts of the information are not absolutely sure but are subject to assessment, to uncertainty? How do you handle that?

McManis: That's a superb question, and the importance is in the question, because I don't have the answer. As we deal with any stream of information, it will be more or less reliable depending on what it is. If you take a picture, by and large you know that's pretty much what you took a picture of. If you've inferred an analytic conclusion, then you have some significant disparity. Two different people may have come to a different conclusion. I think that you also have the problem of synchronism of information. What's the time frame? If you have two different streams of information and they're this much apart, you may be getting a totally false picture. So there are a number of issues like that which clearly have to be addressed, but the question is extremely important. As we develop these capabilities, we have to keep asking the question and trying to find a way to handle those kinds of areas of uncertainty.

Oettinger: Let me respond to that, if I may, somewhat in parallel, but differently. I agree with you that the question is not only a good one, it is perhaps the most fundamental question in this whole business. What is odd about any discussion of information-related subjects is that while everybody thinks they know what they're talking about, it is in fact a subject which remains fundamentally dark and very mysterious.

There was a period 30 or 40 years ago when the things that were called information theory and so on were born, when there was a good deal of mostly scientific and technical activity worldwide associated with seminal names like Claude Shannon and others. It developed definitions of information and quantity of information and so on which were extremely useful in really bringing about this technological cornucopia that we're talking about. All these systems that are now routine computer and communications systems have their fundamental, scientific, and technological base in the ideas that people like Shannon and, before him, Nyquist and so on developed in the 1930s and 1940s and early 1950s. Then the thing died, essentially, as a field of inquiry because extensions beyond that purely technical realm just were not forthcoming. There were masses of papers written, most of them total garbage, about "Information Theory and ..." and you could fill in the blanks; "Information Theory and God." It all amounted to essentially garbage.

These fundamental questions of the validity of information, of the quantification, of the total quality, etc., etc., are not a lot better understood today than they were then. Let me offer what is the one element that I think has some merit that I have distilled for myself out of that period and out of the years intervening which is I think germane to the question that you've raised. That is that the value of information, the authenticity of information, the quality of information is at best a relative concept. The notion of any absolute measure, of any absolute scale, is probably hopeless. I think your example is one of a number of illustrations that I would use to make that fundamental point. You may think you know it and to you it is knowledge. Now, you give it to me. If I know you, or as you say, I look at the signature first

and I say "That's reliable," I will treat it as knowledge for myself. Suppose I have 16 different sources, all of them signed, but there are people I know, more or less, and they disagreed with one another. Whether I'm the director of the laboratory or the Commander in Chief or the CEO doesn't matter; there are 16 people who are giving me stuff which they say is knowledge, and to me it is data. It's just raw, worthless, material that I've got to evaluate starting from scratch.

My sense is that at every level of a hierarchy or in any interchange the measure, whatever it might be, is specific to context, and that therefore this question of how you distill, validate, and so on, probably has no intrinsic answer. Therefore, when we go back to that possibility of surprise or of absence of knowledge or whatever remains there, the notion of an unbroken chain of validation and of value added strikes me as very, very unlikely, because whatever may have happened before kind of gets reevaluated the minute it leaves one person's head and goes to another person.

McManis: The idea, though, of an event sort of happening in isolation doesn't happen very often. There are all of the other things that are related and I think it's particularly true in the development of foreign policy. Foreign policy is not just a President or a Chairman sitting in his office passing out dicta. It really is a process that involves lots of people, the entire structure to do things. Certainly military command and control of all things is a heavily interactive bureaucracy where it is difficult, if not impossible, for a single event just to happen in isolation. So it's not just looking at the validity of a single event, it's looking at the validity and credibility of lots of things going on. From those you start drawing conclusions and that gets me back to my optimism with the warning process.

Oettinger: If all those are embedded in one common central false assumption, then the whole coherence of what you have described is, in fact, its own worst enemy.

McManis: I guess that holds up on the surface. I'm not sure whether it would be valid if you scrub that and put it into a practical case. Have you made the assessment of every event that's happening on the basis of a false assumption, or have you challenged that? I just don't think we do things that way. If you can think more strategically then it seems there's too much involved in the process. If you're down in D.C., and this is what we talked about at luncheon, and someone walks in, pulls out a gun and shoots you, that's an isolated kind of event and the only assumption you can make is that you probably shouldn't have been in D.C. in that place at that time. If we're talking about Soviets launching an attack, which is the other extreme, you just don't do that in isolation.

Student: There seems to be some excitement after the videotape of translating ideas or words into some sort of visual perceptive system that a decision maker can absorb and digest much more rapidly to make decisions. This idea seems to me to have an inherent danger. I see again and again in examples from the business world through psychology that when you've got such a simple display that seems to give you so much information you tend to perceive it in a way that will fit your expectations.

McManis: It gains credibility just because it's so well done and well presented.

Student: And you'll see what you want to see in it. I recall a story that's a little simplistic but I think illustrates it very well. Two rival Cub Scout troops were sent out on a contest to see who could collect the most jelly beans and when they both came back the psychologist who was working this particular test took one group of the Cub Scouts and divided them into two groups. He took half of them into a room and showed them a picture of a jar of jelly beans and said, "This is what your group collected. How many are there in this jar?" They way overestimated it. Then to the other half he said, "This is what the other side collected. How much is there in this?" It was the exact same picture and they way underestimated it. So they were seeing what they expected to see; exactly what they wanted to perceive. If you start translating like that, like these pictures mean nothing to me, you'd have to have an extremely well-trained person to absorb that kind of data and digest it, and still they're going to see what they want to see in it. Something like that.

Ernst: The kind of information that you can test with experiments, so that you can understand the relationships and which ones are more valid, would be hard to find at the national security level.

McManis: Your concerns, just like the other concerns, are absolutely valid. There's still no Holy Grail out there that we can try to find. Those are issues that I had to deal with every day in the warning business. Just with the way we're doing it today, those are problems; problems of perception lead you astray constantly. The problem of media; I used to talk about how do you present the President with critical information so that he reacts to it. If he sees the same format once a week or once a day or what-

ever, the alarm has disappeared, so I suggested that you invent a microchip that says, if you put that warning message on his desk a miniklaxon sounds and he knows that is the one he has to pay attention to. That's nothing on the credibility of the information; it's the medium that's conveying it. Today you have to worry about those issues. I don't think it means you don't try to find some answers to the display of information problem. It just says, "Remember, there are a lot of pitfalls along the way."

Student: If in the intelligence business, when you study that process, one incident that generally comes up as a success would be the trackdown of the *Achille Lauro* hijackers. From public knowledge I know that the NSA had a role in signal intercept and stuff like that. I wonder if you could talk a little about that from within the broader context of lots of pieces of data and what were the ingredients of the human dimension that formed the connectivity between the inputs that led to a decision?

McManis: I really can't get into the details of this for classification reasons, but in a sense an investigation after the fact, after the crime, is perhaps an easier thing to handle. You look for the evidence and you find a clue here and you start going down this track. Trying to do this before the fact, trying to anticipate a certain hijacking or something, is very hard unless there is a whole lot of serendipity. You may just happen to come up with that clue or that source that gives you the information, but that doesn't happen very often.

The other approach to an analytic problem, and that's what the intelligence community does today, or should be doing, is to take this incredible maze of jigsaw puzzle pieces that are just dumped into boxes and scattered around the community, and then somehow try to make a picture out of all those pieces. So, the more your analysts work together, the better that happens. In terms of intelligence failure, most of the big intelligence failures we think about, like the Czech invasion and things like that, were not the failure of absence of information. The failure was in either the analysis or the inability or unwillingness either to sound the alarm or to hear the alarm. That's one of the toughest issues we probably still face in the government. You don't like to say, "The Russians are coming," unless they're already knocking at your door, and the decision maker doesn't like to hear that the Russians are coming. The failures that come to mind were all the result of that. The information was often there, or at least sufficient information to give you ambiguous warning which, in many cases, should have been enough.

Student: You said earlier that speaking from a strategic point you're an optimist. You used the words, "Our primary adversary is much more understanding." I assume that means the classic East-West confrontation. From a national security standpoint, I wonder if the East-West classic is still our primary adversary, and throws out topics like the economic decline of the United States possibly as a national security problem, espionage, or even terrorism. You spoke about how can you ever predict whether an airplane is going to blow up in mid-air or whether you'll be shot in a restaurant in Washington. Shouldn't some focus also be directed toward that?

McManis: Absolutely. If I were in indications and warning today, and anyone asked me, "What's the biggest thing you want to worry about?" I'd say, "AIDS." There's not much you can do about that from a warning standpoint. I think five years ago when I was here I said, "The economic problems that we're running into." Still I think our primary adversaries today are the Soviet Union and the Warsaw Pact, but that's a simplistic statement. Clearly the problems of narcotics and drugs are demanding more attention from all of us. At the rate we're going that will just soak up all of our capabilities. Third World instability will always remain a very significant problem, but you can only focus so many resources on it. You just can't overpower that one particularly. Clearly, there are a lot of other issues involved there.

Student: You were talking about the large amounts of information that someone has to sit down and go through and analyze. Today you hear two sides of the situation. On the one side you hear people talk about the centralization of the analysts, and the fusion in the Washington area at the national level, and then supporting the military commander. You also hear the other side of the issue which is that because things happen so quickly the military commander out in the field, for example, needs to have this information fused or analyzed at his level. Coming from the Washington area, how do you see that balance? Is there an issue, are we going to go to one side and stay there, is there a constant balance going backward and forward?

McManis: There's a constant swing between what you do at home and what you do in the field. The criticism by the battlefield commander is lessening because we at the national level can indeed get things to them in minutes if not seconds. Clearly with his own battlefield resources, while he doesn't need some, they should be focused just on the battlefield. He can't afford to have the total spectrum of

capabilities under his control. I think in the community we're doing a better job of supporting the battlefield commander and we've paid a lot of attention to that over the years. As the commander is becoming more conversant with what support he really has, he's feeling much more confident. He has to realize too that he may be the battlefield commander, but he isn't really in control. When it gets to significant decisions, for good or for bad, they're made in the White House.

Student: Do you see a problem involved with the White House trying to manage two or three crises at one time? Would the President possibly arrive at the point where he must delegate to the tactical commander?

McManis: When we have multiple crises, we're talking usually of Third World areas. What's happened traditionally is that you just ignore anything beyond the first two, and for some reason nobody gets terribly excited until we have time to focus on them; then we get all excited. It's a weakness.

Student: But isn't that saying that we at the White House want to own all the crises and we're not going to give them up, and we're going to let crises go because we don't want to surrender authority?

Ernst: They're not crises until we say they're crises.

McManis: That's awfully close to being the fact. Also, it depends on people, too much, in fact. If you have an Ollie North, he wants to run the crisis. Other people say, "No, let the system work. Let the military command do what it's paid to be doing. We don't have to make every decision." I've been on both sides of this. I was down in the White House when I was the guy who was moving the forces around I Corps in the sandbox. We sent orders out every day saying, "This is where we want your forces to deploy." It's absolutely crazy to get down to that kind of level of detail, but that's what we were doing in the Vietnam War. There were others where we said, "Hey, JCS, go do your thing." I've seen them do some really dumb things.

Oettinger: In the way both of you put it, particularly in the way you put the question, there's something fundamentally wrong. The way you put it was in terms of giving it up or letting it go. I think it's backwards. Dave was closer in pointing out Ollie North. The normal state is that where whatever it is is handled either by nobody or by whoever is routinely dealing with it. It usually takes a positive act, a crisis creation, to pull it up to high level, rather than its being at a high level and let go of. So it seems to me that you're warmer if you put the question in the terms, "Under what circumstance does it make sense for a higher-level decision maker to pull something in?" The baseline option usually is, "Let the goddamn thing sit wherever the hell it is and pay no attention to it." That also is prone to error. That notion that somehow every moment everything is controlled at the center or at the top and then has to be let go or delegated, I think is sort of a false picture of the world most of the time.

McManis: Absolutely. This gets back to where we don't want to have that kind of efficiency where the White House is going to grab every crisis and manage it.

Ernst: The Russians have tried that in their economy, and it doesn't work.

McManis: That's right. They've tried the same thing in their military command and control system, and they have some difficulty when they have to respond so quickly.

Oettinger: I think the real issue is what does one do. This gets back to where the technology has nothing to do with it, but where the perception in the mind of the maximum leadership is very important. So how do you make the judgment when to pull it in?

Student: Except the technology allows the White House to get the instantaneous picture around the world, for example.

Oettinger: What has happened as a result of the technology we're talking about is that the range of options has vastly increased. Therefore, questions about exercising these options are now real questions, whereas even 40 years ago there were no questions. You sent the guy out there and that was it. The famous instances in the War of 1812, where battles were fought after the peace had been signed, are inconceivable today.

McManis: The government today, although we don't do as well as we should, does look out beyond today's crisis. We have institutionalized the process of looking out at the warning crisis that's six months from now, nine months from now, a year from now. That does an awful lot to get you prepared to handle it if it does come or, better yet, it helps you to modulate your response early on so that crisis never takes place.

Student: I've been thinking a lot about this recently in connection with my research paper on rules of engagement as what I call the lynchpin of civilian primacy. In effect, I've come to see rules of

engagement as a method of prepositioning civilian decision-making criteria for hostile response at the operational level so as to ensure that this link between foreign policy and armed response is never broken. If you continue to assume that armed response is nothing more than a method of implementing policy, then it seems to me that one cannot take the risk of separating the two, and so what you have is our rules of engagement which on-scene commanders should use only if there is no time to consult with the civilian National Command Authority. So if you have a developing scenario where, in fact, there is clearly time to consult, then why put the onus on the military commander to react in a sort of vacuum where he does not have an opportunity to consult? All the military officers that I've talked to on the Joint Staff and both the Navy and Air Staffs have concurred with this: that there is no resentment among senior officers about having to consult if there is time.

McManis: That's absolutely right. However, you've talked to the carrier driver who says, "Anybody who pulls the trigger against me, by God, I'm going after him without thinking twice about it." Yes, that's a very valid point. Again, the communications created allow us to have that control in a reasonable way that's not inhibiting.

Student: But the danger, I think, is in assuming that this is a crippling requirement — to have to consult, and it's not.

McManis: Not at all. I feel it can get carried to extremes where you talk about someone moving forces in the field from the White House.

Student: Yes, you can carry it to extremes, but the danger is focusing on the extremes.

McManis: Yes, that's right, always.

Oettinger: I hope you carry that through in your paper and talk about striking balances, if I may grind my favorite axe. You paint the one extreme of consultation as bad and describe what that leads to. If everybody starts consulting, you have the various echelons upstairs overloaded.

Student: You also inculcate a kind of bureaucratic timidity at the lowest echelon where there is a fear of taking action.

Oettinger: So you've got another few weeks in which to think through a little bit of what would your advice be to the commander in chief, the guy in between, the guy on the firing line, about what should go through his head in striking a balance in a particular situation.

McManis: The issues that we've at least touched on around here, ambiguity and perception, will play such a horrendous role in all that.

Student: There's a good deal of just plain risk taking in all of that.

Student: An interesting addendum to your argument here is when you say consulting with the civilians you almost embody "civilian" as a decision-making individual. The danger I see in consulting with civilians in every situation or in most situations, even when it's available, is that the decision maker is not a single individual, especially in a democracy such as ours, but tends to be an incredible political process where there are a lot of different factors and the decision makers have a diverse set of interests. If it was up to that one individual, the Commander in Chief, the President, he might prefer that you not consult because if you consult and he has knowledge then he has to go through the democratic process of consulting his consultants all the way down, and you get a very bastardized type of process.

McManis: We're talking here about pulling the trigger.

Student: We're talking about operational decisions.

McManis: Yes, that's right. There the chain of command is relatively simplistic and the responsibilities are well delineated.

Student: Well, in a short term sense, I'll agree with you.

McManis: But for other kinds of crises, which get beyond rules of engagement, absolutely. We do get bogged down in a bureaucratic process at times.

Student: It's not so much a bogging down as the response of Congress after the presidential use of power imposing limits of 90 days and various other things. These are political processes that even affect the short term. Very line-type decisions are being made.

McManis: I'm not so sure about that.

Student: Just one small thought on what you just said about this notion of bureaucracy tied to the notion of centralized control. The fact of the matter is that in every situation in which nonresponse becomes an instrument of foreign policy, there could never have been a precedent for it in its entirety. Every situation is new and every situation seems to provide a new test for whatever systems of command and control are currently in effect. So, you know, this just supports this consistent theme that I

certainly have come to believe in from listening to this course.

McManis: You're absolutely right. I've had 20 years of being in the hot seat, I know. I've always said, "I may have fixed what went wrong last time, but I'll find a new way to screw it up next time." The circumstances are very different. We keep learning and the way you learn is by going through those experiences. During the 1960s and 1970s we had more than our share of those to keep us well honed. Today we don't have those anymore. Where do you get that knowledge? How do you impart that knowledge?

Oettinger: For the sake of balance, let me turn around and play your earlier role. You're giving away too much now, because what you've just said is true for the little crises that are statistically and structurally unpredictable. I think there's a great deal of importance in what you said earlier when you took me to task on my other comments because when something is massive like a strategic United States-Soviet confrontation, there are an awful lot of things that have to be put into place and I think David's point is that warning and indication, etc., etc., in such a situation are not unreasonable. The alighting of the next fly on the nose of somebody is inherently unpredictable, although one might make statistical statements about there being a greater likelihood of flies landing on the noses near a garbage dump than in a refrigerator, and so forth. This brings back the point about distinguishing scale of conflict — from terrorism to nuclear confrontation and so on — because earlier it was suggested that maybe, if you put enough assets in, you can do a better job of predicting or giving indication and warning on terrorist attempts or one thing or another. It seems to me that I almost buy your point about nuclear or massive strategic confrontation but it doesn't seem to me that that the hope is even there on something which is statistically unstable.

McManis: On terrorism, for instance, I would agree with you, although I think where I would put the resources would be in detective work which is almost after the fact to try to track down people and try to identify who they are. It won't give you warning, but it will help you find the culprits.

Oettinger: That may have a deterrent effect.

McManis: That's right. The experience over the last four to five years in the U.S. government is that is having some effect. The events that don't happen never get reported, but there have been events which have been foiled. There has been much better knowledge about who the bad guys are, what their networks are, how they communicate, how they interoperate, but so much of it is still such an unstructured type of activity that it's tough.

Oettinger: But I think the importance of what you say is that affecting that level of terrorist activities is a reasonable goal. Within a given level, or whatever it might be at the moment, affecting the individual act or localizing or predicting it strikes me as clearly very difficult, if not impossible.

McManis: Absolutely.

Student: I thought your comment about Mr. Casey and his uniqueness was very interesting. I was wondering if you could elaborate a little bit on that. After he died, as I recall, after a short decent interval, he was vilified in the press and someone who had worked closely with him wrote in the *Washington Post*, I think it was an op-ed article, that he had the unique capability to sort of guess what was going to be on the agenda in the White House six months hence, and he would get his people working on that.

McManis: He was predicting the agenda.

Student: He was also, I think, very big on asking his staff, "Why don't you people read?" and he would bring in literary and artistic things outside the normal mode one would expect. You implied that he or he and you or Toomey and Van, or whoever, were sort of unique in that regard but then that ability sort of fell down. You made a quick statement today that you thought it was coming back or was getting better. I was wondering if you would elaborate on what you mean and why.

McManis: Casey, as you described, had some things which I thought were some of the good qualities. He obviously had some qualities which we would not consider totally good. But he had a willingness to look for new ways to obtain information, and he saw the intelligence process as a warning process. That was the reason why he thought we were all in business, to warn of hostile or harmful acts to the United States, and I think he did a superb job of that.

He was constantly trying new methodologies for doing that, of which the A-Team, B-Team kind of thing was one. Some of these were good; some were bad. He knew when they were bad before anyone else knew and he'd walk away from them very quickly. It was his continuous drive to get alternative analysis. He set up the National Intelligence Council, made up of senior government and outside folks too, to be able to take that different view. In terms of making those decisions, he wanted to have people who were broadly read, understood different disci-

plines, and asked naive questions about things that good old Joe, the Russian analyst, would know the answer to automatically. I think that continued questioning on his part was one of the very strong qualities. We were trying to predict what was going to be on the plate at the White House six months, nine months down the line. Our track record wasn't bad. It was kind of the first time we'd ever looked beyond today's newspaper or even a week or so down the line to try to get people to focus on that. So in that regard I think he was very strong.

When he died, a lot of that was left. The strength of the National Intelligence Council sort of diminished and it became much more a run-of-the-mill bureaucratic activity instead of really driving and prodding and being nasty to the rest of the community. I think they are trying to get some of that back — the NIC has been reinvigorated. We're starting to see a little more of the alternative analysis coming back into play now, which I think is good.

Student: It's happening on its own or ...?

McManis: No, no, there are some new players in key places who are trying to stimulate some of that. I've worked behind the scenes for a long time trying to keep some of that alive.

Student: I want to pick up on these different threats to U.S. security, and especially threats to the economic competitiveness of U.S. industry. What uses of intelligence resources have been made towards helping your international competitiveness, if any, or is there space for using your intelligence resources in helping your competitiveness?

McManis: I have to think if I know an answer before I decide whether I can give you the answer.

Oettinger: His paper is on what Spain should do by way of providing economic intelligence.

McManis: I guess I'll give you sort of a soft answer. I really think there's been a lot of talk about what can be done in terms of economic intelligence to the advantage or disadvantage of someone. I guess I have yet to be convinced that we collectively, including our allies, have been able to do a lot with that. There are probably some notable events on every side that you could point to. There still remains, certainly in the Western world, despite some problems, awfully good sharing of information, and thank God we can't identify the critical activities when they're in the basic research stage, because then we would say, "I've got to classify that." So you start the research and then there would never be any sharing and I think we would lose the tremendous dynamism that goes on. So, I have trouble grappling with that as a horrendous advantage or disadvantage either way right now.

Oettinger: Amplify a little bit on that because of the earlier question on that score, "Why is the United States so free about giving stuff away?" I think it has a lot to do not only with ideology but also with size. I think over the years that for a country this size, the balance between secrecy versus the outside and screwing things up domestically is that on the whole it is better to err on the side of being efficient domestically by sharing, because through shared information, decision making is diffused. You don't have to have centralized this, so people can interpret it any way they want. The mistakes get buried quietly in the free enterprise system instead of being matters of public recrimination at a political level, and so if some of it spills outside it is a relatively small price to pay for the internal value.

I think some of the reexamination that's going on, sometimes somewhat clumsily (and that's been a concern), has to do with the reexamination of whether, in the world as it is today, that judgment about where the balance is or whether it needs to be moved somewhat is still a valid one. I think clearly the climate is a little bit toward more restrictive. But there are those who then say, "Well, you're going to hurt the U.S. military, economy, whatever, more by doing this than you'll hurt anybody else." That's what I think the debate was.

McManis: I think so, and I think the alternative answer we're trying to give those people who are concerned about the information is that for those things that are truly sensitive, keep them out of those databases to begin with. Let's think about it at the earliest stage and not get too carried away.

Oettinger: We're going to have to adjourn to get you to the airport. David, many, many thanks!