INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

Warning as a Peacekeeping Mechanism
David McManis

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

February 1985

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

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

Warning as a Peacekeeping Mechanism

David McManis

Mr. McManis is the National Intelligence Officer for Warning and Director of the National Warning Staff where he is directing improvements in information exchange, warning reporting, and relevant underlying technologies. He is also President-elect of the National Security Agency's Computer and Information Sciences Institute. His previous experience includes Chief of the Policy and Management Staff at the Telecommunications and Computer Services Directorate where he was responsible for liaison and support to both the House and Senate Intelligence Committees and the Executive Offices of the President. Prior to that, Mr. McManis worked for the National Security Agency which he joined originally as Arabic Voice Transcriber. From 1969 to 1974 he was Director of the White House Situation Room and a member of the Senior Staff of the National Security Council, providing the President and his Assistant for National Security Affairs with current information on international events.

I think my perspective on the approach we're taking to warning today is a very different one. Let me tell you how I came to be where I am and what it is I'm doing.

At the beginning of this administration Bill Casey was named Director of Central Intelligence. He had a pretty decent background in intelligence. Most recently he had been a member of the President's Foreign Intelligence Advisory Board. He had had a very exciting career during World War II as part of OSS, so he had an old cloak-and-dagger interest in the profession. In particular he brought with him a concern about warning.

After conducting a study group, he decided to establish (or reestablish) a National Intelligence Officer for Warning. It would be a full-time job, not dual-hatted as it had been in the past. And that National Intelligence Officer would work on problems of process, not substance. If you have read my biography, you know that I spent many years in the crisis management business. Very candidly, I wasn't about to go into a job where I saw a big target being painted on my back, so that the next time there was a failure they could say, "Fire McManis and we'll solve the problems." That would not be productive for the system and certainly not for me. So we really did agree that we should work the problem of process. I was also assigned a small staff, which is unusual for a National Intelligence Officer. The grand and glorious-sounding National Warning Staff really comprises only about three and a half analysts today. But again, we're working primarily problems of process.

The first thing we did was to try to decide what we meant by warning. This was a much more complex problem than I had expected. In fact, in my first discussions with Bill Casey I specifically said I didn't want to get involved in definitions. I really didn't think that working that to death would get us anywhere. Yet I have found myself spending more time devoting my attention to what we mean by warning than anything else.

But we've come quite a long way in the last year and a half. Now, when we talk of warning, we're talking about it as communication of a potential threat to national security interests — a communication that is given to the decision maker or the policy maker sufficiently in advance of the event so that the decision maker or policy maker can take steps to avoid or mitigate the threat's consequences.

Now, what does that mean? A little bit of everything. It means concern about the technology, the political developments, economic developments, the whole nine yards. We are trying to get away from what we've been living with for the past 43 years: the curse of Pearl Harbor, which has caused us to focus almost exclusively on the area of military capabilities and surprise. There are scholars today who consider surprise to be inevitable. Well, it just isn't; it's inevitable only if we let it happen, and if we view the world very narrowly in an exclusively military context.

So the message we try to convey is that when you talk about threats to national security interests, you really have to start perhaps two decades earlier, with basic research — breakthroughs that can lead to new weapon systems or other technological developments that can eventually have some economic impact on the United States. Then, coming down the time spectrum, we start talking about the political situation within a country — has a country chosen as its political goal the overthrow or containment of the United States?

Then you have to worry about economic factors — what is that country's ability to wage military war or economic war against the United States? What is the relative importance of the Soviets converting a truck manufacturing plant to tank manufacturing? That has fairly significant indicator value. What aspects of the economy can either help a nation go to war or keep it from going to war? Did Argentina take on the Falkland Islands situation because of economic reasons? You have to look hard at those kinds of issues: problems of instability, both as a precursor to war and as an inhibitor. You are looking at terrorism, narcotics, a number of other things.

We view all these things as a process: political and economic factors, technology — among the things we have to look for first before we finally get down to military capabilities. Then, if we see the capabilities changing and developing, in the context of all other activities, we can begin to divine the intent of the enemy.

Perhaps another way of looking at it is to think of a gigantic jigsaw puzzle moving through time and space, with all the pieces scattered. You reach out for a few pieces — different nations, different kinds of intelligence, different disciplines — and somehow if you pull together enough pieces you can begin to see the picture. If it is a Jackson Pollock jigsaw puzzle you are in real trouble; you are going to have to have an awful lot of the pieces before you know what you have — but in the more representational situations, it may be a lot easier.

There is a major information problem here, a problem we have to work by identifying, and synthesizing all the data. We try to convey this concept of warning as being almost the totality of what we do in the national security community.

How does that differ from the intelligence community? Even within the intelligence community you don't necessarily look at your job thinking about implicit threat. That is particularly true if you are working scientific and technical intelligence. It is only in political and economic areas where threat comes up and clubs you. Military analysts tend to look for an implicit threat, but those in the other disciplines do not. So there is something distinct about putting on your warning spectacles to look at the broader problem and trying to understand what it is you are looking for.

You are indeed looking for a threat implicit in the material you are working, but just as important, you are thinking about the impact of that information as you shoot it out the door. Half of the warning equation is the recipient: the decision maker and the policy maker. We in the intelligence community have been guilty for many years of periodically opening the door and yelling "Here they come!" and then quickly slamming the door, not even worrying about whether anybody on the other side of the door heard the message. I am stressing to our analysts and to the mid-level managers that they have a responsibility to identify who has to hear the information, and then to put it in a form that is usable, understandable — maybe even tailored to the recipient, particularly the more naive recipient. That is a lot of responsibility.

Now, that is a hard message for the mid-level intelligence analysts to walk away with. They say, "Gee, me worry about that getting to the President?" Well, they have to, and we are discovering ways that that can be done.

Student: You are describing a wide spectrum of symptoms. Is the output on the threat side always that you are considering the symptom's military threat?

McManis: No, it could just as easily be economic threat. It could be technological surprise. If the Japanese really do develop this fantastic new fifth-generation computer, totally taking the wind out of our sails, that would be a threat, that would be a warning activity. So would an energy breakthrough.

Student: You also used the expression "economic warfare." Could you clarify the definition of "economic competition?"

McManis: Economic competition clearly has a much more benign meaning than warfare. In economic warfare we are thinking of literally taking on an aggressor — or a target country is economically taking us on in some field.

Student: Is a fifth-generation computer part of economic warfare?

McManis: No, I wouldn't view it as such, though there are others who could answer that better. Economic warfare could include significant undercutting of the U.S. market in production of television sets. That is an aggressive action with some harmful implications. Competition tends to be much more mutually acceptable, mutually rewarding, stimulating. I hate to put too fine a point on it.

We've talked about the doctrinal aspect. Now how do we get the word out? That has meant spending a lot of time in the educational process. We are devoting a good bit of our energies to developing warning training that goes far beyond what we see today within the Defense Department and elsewhere. We are addressing the problems in much greater scope, trying to find ways not just to get to our intelligence community, but to get to the decision- and policy-making community. We hope to have Foreign Service Institute courses dealing with the problems of warning, slanted toward future policymakers. One of the alumni of this class is deeply involved in that with us.

Another area we are trying to illuminate is all the paradoxes of warning. We don't understand them well; there is a lot of room for more research.

An example of paradox is that the earlier we try to provide warning, the more ambiguous that warning may be. And ambiguity is hard for our decision makers and policy makers to cope with. It is particularly hard because for so many years we talked about unambiguous warning. From my viewpoint, the only unambiguous warning today is when you see that the missile has been launched, or the bullet has been fired and is on its way toward you. That sure isn't much warning.

So it becomes incumbent on the decision maker, the policy maker, to understand that problem, and this is very difficult, for instance, for the Department of State to accept. They want to have one nice neat scenario against which they can plan. I don't blame them. It would be very nice. But these are the words we usually have to use: "On the one hand this may happen, but on the other hand that may happen."

We have to find ways to express these alternative scenarios — particularly when the "judged-less-likely" scenario has much greater threat implications for the United States. Indeed, it may be necessary for our State Department, our Department of Defense, and the White House to take steps against both alternatives. That has resource implications — one of the primary reasons it is not very popular — but we are still stuck with it.

The trade-off against ambiguity is timeliness. The closer you get to the event, the more certain your judgments and information become. You have to warn of an event in relationship to its timeliness.

Another paradox is a problem we deal with constantly in our estimative work: consensus versus sharpness of decision or analysis. For years and years we based our estimates on consensus, coming forward with a draft position that was massaged by a roomful of intelligence gurus until it had little or no significance but certainly was not offensive to anybody. We have had to find ways to get away from that. And even though our estimative process today still uses consensus, we have encouraged alternative analysis, development of alternative scenarios, and publication of dissenting views. So no longer do we feel compelled to go forward with the national estimate which has only one — usually very safe — view of what the future may bring.

Furthermore, the organization I represent, the National Intelligence Council, and the other 16 National Intelligence Officers, are instructed to look at developing situations in terms of their possible

alternatives. We are asked to look under the rocks and see if any views have been overlooked. Periodically we are asked to play devil's advocate and develop detailed alternative scenarios to be bounced off, and perhaps even to wake up, the community. So there is an active effort to look at the other side and make sure that we are not guilty of falling into the trap of consensus.

Another difficulty is inherent in analysis. You go into a problem trying to discover truth. You work your way through it, collecting all the evidence, and you put forward a brilliant exposition. Now having gone through all that pain and soul-searching, you have become so wedded to your viewpoint that you will never question it, never go back and ask yourself what is wrong with it. I think we have all been there. It is a very hard failing to avoid. Even though we warn our analysts that this is going to happen, and not to let it happen, it happens time and time again, and I am not sure we will ever totally overcome it.

Even worse is when you go in with your mind already made up, and collect evidence to suit your particular hypothesis. That is very damaging.

Student: Could you insist that an analyst cite deficiencies in the analysis, cite lack of evidence, or whatever the gaps are?

McManis: We do that. We try to identify in the analyses, where appropriate, what will be intelligence gaps, or inadequacies in the information.

Student: It is very simple to say, "I didn't have enough data on that point, so I am making the best guess I can," but that's not what I meant. Not just gaps in the information that has flowed to the analyst's desk, but inadvertent or unavoidable gaps in the analysis, because of the structure of the problem, let's say.

McManis: If analysis were more of a science and less of an art, maybe we could do that. Something of the kind may be done, a little, in the normal analytic review, not by the analyst but by his supervisor, to try to point out the flaws in the analysis. But working an intelligence analytic problem is not quite like developing a series of equations, where you can really look at the facts in a neat little package.

Oettinger: How does that tie in with your earlier statement that, contrary to what some believe, there need not be any surprises? It would seem to me that the discovery of ground truth has meaning only at the end, and can only take place after the fact. So if the analyst is to ask, "What should I have known? Is the analysis complete or do I need more?" — in what sense can that be done?

McManis: That leads me into the next area I want to talk about: how we cope with the information we have. We have become, technologically, an extremely competent collection mechanism. Our intelligence resources today are phenomenal. I can't go into them, but I can tell you they are phenomenal. If you read *Aviation Week* you get some appreciation for them, and you have to think of what the Soviet Union thinks about them.

They are really good, not only because they are so sophisticated, so much like vacuum cleaners, but because they are varied. They give us lots of different ways of getting at our problems. They are not complete, certainly, and no intelligence analyst would say, "Collect less for me." But we are doing so much. And our problem has become one of having literally more data than we can possibly convert into knowledge. We have to work on that part of the equation, and I think that is where we can work toward avoiding surprise. Again, the more pieces of that jigsaw puzzle we have, the better off we will be in divining the picture.

Most of our post-mortems have shown us that the information has usually been there. It has not necessarily been pulled together or synthesized properly. Often it is not recognized. (Often, too, the decision maker didn't want to hear that particular message on that day, and so ignored it.) But the information is usually in the data.

So there is a tremendous challenge — not just in the intelligence community, but to the entire information community — to try to exploit what we have. We are spending millions and millions of dollars each year collecting information. There is also the whole world of open source material, which we are not close to exploiting fully. Putting those two together makes your problem worse, but it makes the opportunities even greater. The challenge is to somehow convert the bits of data into knowledge

bases without having thousands of trained monkeys sitting at their CRTs entering the data and trying to recognize and identify it.

Oettinger: But how can you claim that you are eliminating surprise? It's true that the data are always out there, the phenomenon is going on — but whether it is just out there or we have made an observation and it is in our computer, either way there is a fundamental scientific, analytical, scholarly, etc., problem. If you are staring at the data and you don't see it, that surprise is in part a problem of perception. That was true even in the Pearl Harbor analyses, Roberta Wohlstetter and so on. The information was there, but people either didn't see it or they loosely interpreted it into something else. So what's your argument with that? Is this Richard Betts' viewpoint? It seems to me that, from a perceptual point of view, surprise is possible.

McManis: Well, what we think is perception is a process of trying to evaluate that information you are seeing, those anomalies — not just in terms of the military threat, but to understand that the target country really does have some interests inimical to ours, that they have taken the nonmilitary preparatory actions that would allow them to go to war.

But I don't think you can do that out of context. Surprise occurs when you have a military analyst looking for military blips on the screen, as an exclusive and maybe even a pipelined kind of activity. We are trying to get the more complete picture which expands in time and depth.

Oettinger: I'd be inclined to agree if you'd said surprise might have been avoided if, instead of focusing only on the military or the technological, we had looked at economics — the Japanese are buying scrap iron, that sort of thing. But I am trying to probe what you mean by *no* surprise. I understand what you are saying, but I don't see it. You are saying that in principle you can get all the data, and if you look at it in enough context the answer is "out there." Logically, yes, I agree with you, there would be no surprise. But if surprise is a mental thing, a state of mind of the analyst and the decision maker in light of the post-mortem, then surprise is possible.

McManis: Well, first, I think that in today's environment, with our advanced collection capabilities and our ability to pulse the world, you can fairly routinely understand what is going on out there. There is much more data on which to base our decisions; we will see a whole series of phenomena which could be related to a hostile event. Having done that, the challenge is somehow to get it all together and synthesize it in a reasonable way. We are doing a much better job at this today, though it is still difficult. But then the final part of the equation is that, indeed, if we do not do a good job of conveying the information to the decision maker, or if it conflicts, or if he doesn't want to hear it, or if he is just not receptive, we may lose our chance to warn him — and he may be surprised.

Oettinger: Well, but to say that surprise is eliminated is as nonsensical as to say that it is inevitable. Surprise is more or less probable. Wouldn't it be better to say that we have means to reduce the probability of surprise? That has to be good enough — instead of making a statement like "there is no possibility of surprise."

McManis: Well, I think we have the means to avoid surprise today, and we continue to avoid it.

Oettinger: I don't believe it. That is so extreme a statement that it seems off the wall.

McLaughlin: I don't think you are doing Betts any justice. First, if we design a system to scan and to try to avoid surprise, we know we designed it for a whole set of conditions. I think the Betts argument is that anyone who wants to try to take advantage of you is going to try to design his threat to avoid your system. To the degree that he understands your system, that may be possible. Such mirror-imaging has to be done very much in the context of a conscious effort to avoid your existing warning system. And I am not sure that all of us are so omniscient in designing a warning system as to be able to avoid that possibility.

Second, surprises are constant. What of the excuse, "The Old Man didn't take my advice." Look at the seizure of the American Embassy in Tehran — that was a surprise. Even though it had already been done 60 days earlier, it still seemed to come as a surprise. The 250 Marines getting bombed in Beirut was a surprise, even though the American Embassy had been hit by a very similar method — even though we knew there were people out there who hoped to

do us harm and who had demonstrated their capability to do so before, the Marine emplacement was taken by surprise. And that was one-eighth of a Pearl Harbor in terms of casualties.

McManis: We are running into a problem of the meaning of the word surprise. You are certainly both right. But I can argue just as well that the bombing of the Marine barracks was not a surprise, even though there were unfortunately a lot of surprised people. It depends on what we mean by surprise. I may have been firing for effect a little bit, but I still prefer to work the side of the equation that says we can avoid surprise, rather than the side that says surprise is inevitable.

Oettinger: But why do you need either of those extremes?

McManis: I thought it was a delightful contrast to make.

Oettinger: Yes, but I think it is dangerous. This kind of polarized rhetoric, you know, gets us in trouble.

McManis: I agree, I will accept that.

Student: A non-American example is one of the other great surprises of the 20th century: the surprise attack on Russia in 1941. Well, it wasn't a surprise — it was coming and everyone saw it but the man at the top. So when I think about surprise, I think about the decision maker at the top who has to give the order to prepare or counter. There may be lots of analysts for whom it is no surprise. In fact, in the Soviet lexicon it is no accident, but Stalin apparently refused to recognize it. It is not a question of getting more information, better information, highlighting it or synthesizing it. It will be rejected if it does not fit with a strong mindset. If the negative mindset is that strong, it will just discard whatever information and analysis you send up. And that is a real problem.

McManis: Yes. I agree, and I think that is why, from our standpoint, it is important to work the other side of the equation — not just worrying about what is shot out the door, but worrying about how well our president understands the warning process, so that he can have some measure of confidence in what is going on. I think those are very critical issues, and we really ought to continue to work them. I would like to think that we have a less naive presidency today than we had years ago, and that next year, and in the next ten years, it will improve all the more.

Student: To what degree do you accept responsibility for communicating that warning, compared to putting that responsibility on the president's side of the fence? At what point would you say, "Well, we did the best we could."

McManis: I don't want to take that approach to the problem. I think, as I indicated, that it is incumbent on those of us who are warners to follow through. We have to consider all the means of warning, including the importance of the media in conveying warnings, whatever they may be. We really can't be sure what is going to get the president's attention. Is it going to be a piece of paper that has a red bar down it and a warning notice across the top? Or a video image that shows the Iranian aircraft going after U.S. ships in the Persian Gulf? Or, as is probably most likely, is it a telephone call from Bill Casey that says, "Mr. President, something bad is going down and you have got to do something about it." All those things are important, but we need to work the problem of the media, and how you convey a broad variety of warning information to the people you are trying to warn. We have to keep from falling into the trap of the warning becoming too familiar — maybe changing the color of the paper, or putting a microchip in the corner that emits a klaxon when it hits the decision maker's desk. I am not quite sure how we do that, but we have to keep working at new solutions.

Student: Are we getting better at synthesizing data? How do you measure that?

McManis: We are working the problem, and we need to do an awful lot more. Right now the opposite may be true: our analysts are so busy processing data and trying to convert it into something useful that they have less time to exploit databases and pull information together.

Student: Let me rephrase. How could you tell that you were synthesizing data better? Would there be empirical evidence? seat-of-the-pants subjective assessment?

McManis: The first way I would know would be if the analysts could access data that they can't access right now. Today an analyst may have to go 20 different places to get a complete view of a particular problem. Probably they are not doing that; they are going to their three or four favorite places, and can't even get to some of those. So there are a lot of impediments to their reaching the information. The first thing we have to do is remove those impediments and make the information easier to get. Out of that, I think, will come improved synthesis.

Oettinger: Your answer to the question is like the Supreme Court's answer to "How do you know pornography?" — you know it when you see it. That's not as much of a copout as it seems, as long as you're not in an extreme, and I'm completely in agreement with it. It's obvious to a supervisor when an analyst is synthesizing from two sources when he's got ten available, and whether he isn't using his sources or can't get at them. The process could be improved. It's not a very deep philosophical problem if the goal is to improve something by x percent. It's only toward the extremes where you begin talking about certainty. It's a matter of improving probabilities; it's not a very statistical process. How can I improve on a synthesis? Perhaps if I have people trained as economists and in political science and maybe some engineering. Am I crazy?

McManis: Not at all. There is another complicating factor. As I said, assuming you have access to all the information, and that you can search all the databases easily by asking a single question, you still have the classic analytical problem of the analyst's willingness to accept or deal with the evidence when it conflicts, or leads off in directions he really doesn't want to go. So we agree that there is no easy way to know it when you see it. I'm not sure I'm quite that relaxed about the problem.

The warning process today is a hell of a lot better than it was in 1941; we all know that intuitively, if not from experience. That does not mean it comes anywhere close to perfection, but maybe we're beginning to start working on the upper margins. I think we have a good system — I want to be very positive about it, though if I were talking to the intelligence community I'd be very negative about our capabilities. We really have a tremendous foreign database.

Student: Do you work with the president, or that group of people you're trying to warn? Do you talk to them about what they need to see to be warned? It sounds like you're always trying to figure out your audience.

McManis: Good point. It's very important that there be a dialogue between intelligence analysts and the policy decision maker. That's not an easy thing to establish or sustain. It tends to be confined to specialists; for example, actual intelligence officers who will deal at senior echelons. Very few of us, if any, have direct access to the president. But we do have fairly direct access to Richard Beal and the rest of the national security officers and Security Council staff who are much more cognizant of the current policy considerations.

Now, they are very careful because of the risk of having policy drive intelligence. As a community, we have to guard against that. It really is rather easy at times to put forth a good analytic judgment which, by changing just a couple of words, can be brought a little closer to current administration policy. We try very carefully to avoid that.

Student: I wish to follow up on Tony's argument. I think I agree with him. I'm uncomfortable with the idea that you can build a system that just won't ever be surprised. One of Betts' arguments was that even the best warning system would be like a batting average: you'd improve your batting average, but you'd know you aren't always going to be hitting the ball. The more you think you're always going to be right, the more vulnerable you are to being surprised in some instance. Instead, the best warning system may be something that is right 40 percent of the time. How do you feel about that?

McManis: I guess we have a basic disagreement. I believe we should continue to strive for some measure of perfection.

I haven't touched on this yet, and I should, in more detail. In the Washington area today there are some 14 or 15 principal crisis management centers. They are tiered. The "big six" of the National Security area are: the National Military Command Center,

which has operational responsibility; the National Military Indications Center, which is strictly intelligence; the State Department Operations Center (operational); State Intelligence and Research (intelligence); the National Security Agency's Operations Center (intelligence); and the White House Situation Room.

The next tier, primarily operational, includes the service operations centers, Army, Air Force, Marine Corps, and Navy. Below that is another tier which is getting a lot more action these days: the crisis centers of the Department of Commerce, the Treasury, the Federal Emergency Management Agency, the FBI, and in terms of nuclear terrorism, the Department of Energy. These people are the front line in terms of crisis containment and subsequently crisis management. We've been working with them to try to strengthen their bonds.

You probably don't recognize how unusual it is to have those people working together — having an operations organization like the J-3 working closely with a bunch of intelligence people, with very few boundaries between them, and complete sharing of information. When you throw in the Department of Energy as another separate but equal player, that's a pretty potent force. Then if you realize what each single node represents in terms of our ability to literally encircle the globe, putting tentacles out to the other military and civilian watch centers throughout the world, it's a damned impressive network.

The problems lie in making sure that the players themselves understand what it is that they have — that they understand the capabilities of their counterpart centers, and know how to marshal all their selective assets to work a crisis without tripping over one another. In the conventional scenarios — nuclear attack or even a nonnuclear event, say a collision of a U.S. destroyer and Soviet submarine, we handle things very well, because we have a limited set of players. But let's say a group of terrorists successfully captures the nuclear generating plant at Hanford, Washington, and holds it hostage. The community responsible in that situation has at least four people in charge, maybe more. How well have they worked out the operating procedures to deal with that problem? They really haven't yet.

We're trying to recognize those kinds of problems and work on them, trying to tighten up the crisis management community. Richard Beal, through what he is doing at the White House in a planning sense, is driving or assisting in that. It's hard for us to tell sometimes, but he is working on those kinds of problems in a very constructive way; so we have a reasonably healthy approach to that aspect.

Student: Has the U.S. made any progress in strategic warning with its allies during the last few years, specifically in solving the NOFORN* problem? How do you see us working with our allies in the future on strategic warning?

McManis: We're working very actively, particularly on the NATO contacts. That's a strange and wonderful world; even though we're working with the NATO context we end up having to work with each country individually. Still, we're trying to come up with the same answer for all. The focus remains very heavily on the military angle: the classic indications of warning problems. We continue to talk about the broader dimensions of warning, and we get various levels of receptivity. Over the past four years we have greatly improved our exchange of critical warning information, particularly with our NATO allies. We still have a very long way to go in that arena, but it's become a much healthier operation.

Student: Is there any kind of conservative bias within the intelligence system? And if so, would that not lead to a surprise when something does not happen, sort of a negative surprise?

McManis: Our track record for estimating what's going to happen over a period of time is not really all that good. And we continue to err on the side of conservatism. We tend to choose middle-of-the-road, and status quo kinds of answers, and we recognize that. It seems a little more sophisticated than saying to ourselves, let's just climb out on a limb each time. As a community, though, especially within the National Intelligence Council (because we're the guys who are supposed to be breaking down those things), we still are not there. We are working that problem exceptionally hard, but we don't have good answers yet.

I'm not sure that's really the entire problem, however. Some things will continue to surprise us, such as the downing of the Korean airliner. We were not prepared for that, even though, if we had postulated

*Code word restricting classified information: no foreign access

a Korean airliner flying over the Soviet Union and really thought about it, some of us could have predicted the consequences. It's a very complicated problem, and I can only say that we recognize it and are working on it.

Student: I was heartened by the fact that you have dissenting reports now; that's a big step. It also seems that training and coordination among the various elements of the community are important to counter the overlapping, redundancy and diversity. It seems you've got it on the right track.

Student: Would you talk a little about the decision support system models you use for intelligence forecasting, particularly after the Iranian crisis? I don't see how you actually forecast the stability of a foreign country and try to figure out revolutions.

McManis: The Central Intelligence Agency is working on that. They have developed a number of models of political instability which count demonstrations and about two dozen other indicators that end up spelling coup d'etat. But it is early work, so we don't rely on it as an accurate forecast. We do much of our national-level forecasting now by having the National Intelligence Officers sit down together periodically and brainstorm, trying to identify areas of the world that could become problem areas. Then we try to say to ourselves, if we think the next crisis may be in the Philippines, are we postured even to recognize it when it comes up?

Student: When you talk of earlier warning, I think of nuclear attack. When there is a nuclear alert it could mean that the Soviets are accidentally attacking us, or that they are deliberately attacking, or that our own equipment is not functioning properly. There are several possibilities. In that short time frame, how can intelligence gathering make any difference?

McManis: Most of us do not believe that the Soviets will or can launch a "bolt out of the blue." They will take some preparatory steps so that they can at least minimize some of the impact on themselves. If those steps are taken, and are identified, that gives you a context; then you can begin to evaluate what you are seeing.

Part of the answer is mechanistic and technological. How good are your sensors — are they still confused by geese flying by? I think, though, that however you answer that, we have worked out those kinds of problems. The problem of Soviet intent will be the critical one. For that we will need a lot more contextual basis for our evaluation. After launch, though, it seems you're right: it's too late to get to General Hartinger, and CINCNORAD, in Cheyenne Mountain, who is going to take whatever information he has and send it right down and say to the president, "There is an attack under way."

Student: I think the "bolt out of the blue" can become confused with other scenarios: crisis alert, or signaling. I don't think anyone who analyzes the "bolt out of the blue" scenario thinks that the Russians would use anything but the alert forces. They would, for the very reason you offered, avoid any signaling that would tip their hand. If they are really going to hit us out of the blue, they are not going to evacuate Moscow first.

McManis: I agree with part of what you said, but we do believe there are indicators that we would see sufficiently in advance of an attack like that.

McLaughlin: If I may reinforce that, that's what I was saying about Betts before. To the degree that the Soviets think we are looking for a particular indicator, they would do their best to avoid it if they want to achieve surprise.

Student: Or they may try to intimidate you, and evacuate Moscow in a crisis to demonstrate their seriousness.

Oettinger: We're lapsing, it seems, into extremist nonarguments. On the one hand, bolts out of the blue don't just happen; somebody will have had to set up a mechanism, train forces, etc. If you go back far enough, perhaps twenty years, there may be first indicators in some open journal of what is now becoming doctrines and plans. If we start looking for this, the whole notion evaporates, because there was no surprise. You are watching, and you have an indication that so-and-so went to a particular post — and that may be sufficient. You can turn that bolt out of the blue into an historical warning type of problem, and thereby reduce the probability of surprise.

On the other hand it is damned hard to stop a dedicated kamikaze from approaching a head of state,

pope or president, and shooting at him. So it is irresponsible to rule out conceptually the possibility that somebody will undertake something as suicidal as blowing your head off before you can blow off his. The notion that there can be no surprise strikes me as intellectually bankrupt.

McLaughlin: With hindsight you can go back, as often as not, and find that the information really was there within your system, and it just hadn't come together, or been seen in context. I couldn't agree more. But it worries me when I hear, "There were surprised people on the ground in Beirut, but it really wasn't surprise." That, it seems to me, is ignoring the purpose of the system. That's the problem of looking at intelligence, or warning, for itself and not for the end result.

McManis: There were failures in Beirut and they were pointed out by the Long Commission, which did quite a good job. There were failures on several scores, and some are classic warning kinds of problems. There was a series of warnings, not only daily but many times a day, saying, "Those guys are out there and they want to blow you up." Part of the problem was the intelligence community's failure to distill that information and get it through in a recognizable way, so that it wasn't just bits and pieces hitting Colonel Geraghty on the ground. Steps have been taken there. Part of the failure was on the part of the operational planners, who said to Colonel Geraghty, "There are some things we don't want you to do, in terms of your profile and where you're going to stay." Part of the problem had to do with Colonel Geraghty himself — failing to close down opportunities for terrorism in the face of a known terrorist threat. So there is plenty of blame to go around, and it's all human failings.

Student: You've been talking a lot about the human side of warning: synthesizing and coordinating the information. Could you give me some idea how our resources now break down between putting enough money into the human part, and putting money into the strictly technological side? Do you think the balance is right? Or do you think we should put more effort into one side or the other?

McManis: I don't think the investment in either the human or analytic side is adequate, not by a long shot. It gets my technical collection friends up in arms to think about putting up one less satellite, but I almost would do that. I really think we have to start investing elsewhere. Part of the technological aspect is that we have to start trying to build the knowledge base: getting the information in usable form, getting it to our analysts, and really working on training analysts. We have had a very significant turnover in the analytic corps in the last ten years. They are a much younger set than we've had in the past, and they haven't lived through as many serious situations as many of us have. That may be good or bad, but they do have fewer preconceptions.

Student: Even though you may practice coordination within the community, what happens when you have trained some people in your way of dealing with the information, and then someone is replaced? Do you have some way of backtracking? Once you have a new person in the position it won't necessarily be the same. When somebody gets replaced, the new person may have a different way of going about it. Some military commanders have talked about how the command and control system can be designed for an individual, but by the time it was used the person it was designed for would be gone, and the new person could not manage the system.

Oettinger: I think the question is, can coordination survive institutionally?

McManis: I'm not sure I have a good answer, but I think coordination does tend to survive institutionally. Coordinated products tend to be reflections of the institution as much as products of the individual, maybe more so. In terms of the management techniques and the approaches to the problem, in crisis management we are trying to create a system that people can move into and out of very quickly at different levels of expertise. We are forced to do that because of the high turnover, and because of the prevalence of people who have not been through the major crises of the sixties.

Student: How much effort is the intelligence community making to gain familiarity with Third World areas from which a crisis might come? For example, when the Iranian problem breaks out and you find you have only two people who can speak Farsi and

nobody knows anything about weather conditions in the Iranian desert, that leads to awful errors. Is anything going on to correct that?

McManis: I'm not sure I can quantify it, but yes indeed, there is great recognition of the Third World problem, and it is being worked extensively. Our number one target will forever be the Soviet Union. We've quantified our resources, and the majority of them are aimed at the USSR. But the crises we get involved in are in the other areas of the world, and we will continue to be surprised and suffer through those problems for another twenty years, and longer. But concerning the problems in the Pacific, in Korea, Japan, the Philippines, problems in Latin America (I'm not sure I completely understand why we have such great difficulty in working those out, but we do) there is very significant attention paid to these problems: analytic attention, collection.

Student: Even before they are problems?

McManis: That gets back to what I was saying earlier. We try to forecast those areas, in my office particularly. I try to identify areas that are not being looked at and should be. At any time there are about half a dozen "sleeper" areas around the world that our collection gauge has been turned away from, but which need to be looked at periodically.

Let me briefly discuss our alerting mechanism. We have many formal ways of sending our warnings. Our principal long-term mechanism is our national intelligence estimate program. We are very active in that program. I think last year we put out 68 estimates and special estimates. In past years they tended to be nebulous, but today those estimates are highly focused in terms of threat implications. They are really the number one warning documents.

A national intelligence estimate is something that six of you might do if you were area specialists representing different departments looking at a specific target country or problem. The presidential succession in the Philippines is an example. You put your best people on it to try to give the president or the National Security Council your best estimate about where that situation is going in the next six months or year, depending on how you define the problem. You try to marshal the evidence, lay out the facts and the scenarios. You say, today, if this scenario is followed, these are the kinds of things we would expect to happen. On the other hand, if you start to see the following things, it's very likely that a different scenario is being followed. The estimate goes through a very formal coordination process; it's blessed by all the principals in the intelligence community, published, and given to the president and the National Security Council.

There are other mechanisms for getting the word through. At the other extreme is the informal method. I want to stress the criticality of the old-boy net. Not only does it exist, it is viable and should be nurtured. There really is nothing better in terms of warning than to have a Bill Casey pick up the telephone and tell the President, "That estimate on its way over to your office represents a very serious threat to national security." That is an attention grabber. It can be done at different levels, too. You can perhaps go to an assistant secretary to get that message through, or even do it at the lower analytic levels. So while we can never say that the informal network will replace everything else, it certainly is reinforcing and we want to exploit it very well. We are trying to recognize that very specific ingredient in the national warning system.

Student: How useful can those formal documents be? How long does it take from the time the analysis is conducted to the time the document is on the street?

McManis: We can get them out in a matter of days, from the time the question is raised to publication and availability. We've done it in three or four days in extreme circumstances. Ideally you're evaluating a situation you're hoping not to face for months or even years.

We're trying to get away, too, from handing in an estimate automatically once every year — revisiting an area just because we haven't done one recently. That's self-defeating, and people don't want to read those.

Student: Mr. Beal talked last week about maintaining files on crisis areas. I'd be interested in knowing the difference between the files you and he maintain. What kinds of information are shared across them? Are you working on parallel sets of data?

McManis: We hope we're working together. The files are the record of the way crises have developed in the NSC context and actions taken on them. They

are unique, they are like a working analyst's files, a compilation of everything that comes across his desk or through his operation. They become a very interesting resource, allowing you to go back and try to reconstruct what really happened. We haven't really had that sort of resource in the past. What we're hoping to do with Beal, in a rather low-key way for bureaucratic reasons, is get the crisis managers in the community to sit down off in the corner and look back at what has happened and what has been done about it, to gain some insight into how we can strengthen our actions. Yes, we are working on that; but there are some sensitive overtones.

Student: Are those files used to anticipate crises?

McManis: No, I don't think so, though Beal is trying to be prepared if they do see something. For instance in the Iraq-Iran situation he's tried to make sure that they have the basic factual information at hand — it may be nothing more than the maps, the order-of-battle information, those kinds of things — so that he doesn't have to make that call too hastily. But his information resources really are the intelligence and operational communities, whom he calls on to assemble bodies of information for transmission to the White House. He is building tremendous, wonderful data bases for the White House. That's as it should be.

Student: He did mention that one of the problems is knowing where the information is in the community. He mentioned northwest Africa, and not being able to find an oasis. Is any work being done to compile central data on where data is?

McManis: Yes. We've taken some steps backward too, because for manpower or other reasons we've done away with some good resources: openly available information sources and lines of communication in countries around the world. We're trying in some very specific cases to rebuild and reassemble those resources for the community. We, the crisis managers, are working very closely with Richard Beal to see if we can't develop the necessary information bases to be prepared for the off-the-wall crises, so that you don't spend six hours trying to find a map of the Falkland Islands. That still is a significant problem.

Student: Who becomes an intelligence analyst? Are they political science majors, or are they specialists in different fields? Is there a need for a special academic curriculum? Is a certain kind of training required?

McManis: I'm not sure you would ever want to rely on one particular source for your intelligence. Political science is a good capability to have. Though I'm from the National Security Agency, a highly technical agency, I am an art history and philosophy major, and I feel that to be a good analyst you must have an ability to see, to be able to distinguish among the ten thousand shades of green — to be able to recognize patterns. I think art historians, artists, or musicians can do that kind of thing. I have urged in my own agency that, as we continue our recruiting program, we hire not just engineers, mathematicians and computer scientists, but art historians, linguists of course, a few French literature majors; they bring new perspectives to the problem. We need to get that collective strength in the group. Anybody who is smart can do well as an analyst.

Student: You have made a couple of generalized statements that seem to be in conflict. Both statements we can all agree with, but I am wondering how they fit together. One is that we need to find ways of getting the warning through to the decision maker at the top. We have to format it correctly, whether it be the phone call from Casey or whatever. On the other hand, you said it is important to open up the analysis to make sure that dissenting opinions can be expressed — it is almost a plea for more richness. I am trying to put that together in my head, thinking of Casey at three o'clock in the morning calling the president and saying, "On the one hand... yet on the other hand..."

McManis: It goes back to ambiguity and timeliness. He is calling the President at three in the morning, saying, "It is likely that something is going to happen at 3:01." Or, more likely, it has already happened. So at that level you probably don't have "On the one hand, on the other hand."

Student: Let's take a daily briefing then. If you are trying to be concise and clear, you are probably missing some of the detail. Usually we have some data

which in retrospect should have warned us, and there were probably some people who were warned and were pleading that that view be expressed. But if you come to the man at the top with a collection of conflicting analyses ... I have seen these things with footnotes and dissenting opinions, and it makes you just not want to read it — or you wonder, what is the real story here, and can't they figure out what is going on, and how am I supposed to know if they don't know? The two generalizations are laudable, but have you thought about how they fit together?

McManis: I guess I don't recognize the conflict. I see them as consistent.

Student: You can't allow too much of "on the other hand," because if you do you risk losing influence. There is also that risk in allowing expression of a dissenting opinion.

Student: But the warning may not get through. There may be too much background noise, or perhaps it is the footnote on page five that is important and the rest of it isn't; and how is the decision maker ever going to focus on the footnote on page five when the rest of it is saying, "There are problems here, but we don't think it will blow up."

McManis: There are some very complex issues in your questions. How do you convey warning effectively to a senior decision maker? In practical terms, one of the things we do in the estimates program and in some of our other intelligence analyses is condense the message into what we call "key judgments," one or two paragraphs that represent the meat of the twenty-page estimate — because we know the President is not going to read the twenty-page estimate. He may have a staffer read it and highlight it, or he may not. But he may well read the key judgments.

Oettinger: But whatever the formal warning system may do, it is only a piece of a larger whole. Beal said it was only a matter of a minute and a half each day. So you are only looking at a piece, and you are only looking at its being better by five or ten percent. Don't fall into the error of assuming that the subject of this discussion is all the inputs going to the decision maker. I can't overemphasize that; nonsense gets generated by focusing on a single piece of a big system. It is just as bad as the old crony's assumption that the decision maker only talks on the golf course, and the hard-to-understand analytical stuff plays no role. If you look at the history of good presidents, or good chief executive officers, they have gotten to where they are, and been better at it than their competitors, not because they are perfect, but because they could plan the various channels better than somebody else. The bottom-up staffer's view that his tool is the only thing the boss uses is one of the reasons why some of us remain staff guys or professors and not President of the United States. So we are talking about our staff failure, rather than about the behavior of the line executive. I think it is critical to keep remembering that. Most of us are here as staff types. If we were line types we would be out there running something, not here in school taking courses or teaching.

Student: I have a doubt about the input of your system. You spoke about tools, and how you can confront crises abroad, but speaking about the inputs you gave the impression that all the inputs come from foreign countries. I think you need not only the inputs coming from abroad, but also those coming from your own country, and don't forget you must relate what is going on in your country with what is going on in, and can happen in, the other country as a reaction or as a consequence of it.

McManis: I think you are saying — and I agree — that we have to go about our process with a full understanding of how we and our actions are viewed by the other country, particularly our adversaries. So that as we take measures and countermeasures we will understand the implications of the signals we are giving off. We really haven't touched on this: perceptions of how everybody else views us and how we view them. Really understanding that is an enormous area, worth a whole session in itself.

Oettinger: Next week Leo Cherne will probably discuss a piece of that: how public perceptions within the United States and elsewhere are shaped, focusing particularly on the role of the media. That is a piece of what you are describing.

McManis: Let me recommend too for reading on this subject a book by Robert Jervis, who is now at Columbia, *Perception and Misperception in International Politics.** It is an incredibly good book, tough reading but well worth the effort.

Student: I was surprised by the reaction of the American public about what happened in Beirut. I think that set of events can be understood by asking the question, "How was the role of the United States in Beirut perceived by possible enemies?" What happened in Beirut could perhaps have been forecast if you started from this point of view.

Student: One of our readings, by Richard Brody, indicates that the Soviet invasion of Afghanistan involved, if not an intelligence failure on our part, at least some lapse in intelligence warning. Yet my perception was that the intelligence community fairly well called that shot. Was there a problem in getting information to higher levels?

McManis: It is hard for me to comment, because I wasn't playing that game at the time; my understanding is the same as yours: that the information was there; it was well analyzed; the assessments were done, and it went out. There was some reluctance to deal with it, or even perhaps to understand how to deal with it.

Student: I was surprised to see it mentioned in the same context as the Czechoslovakian invasion or Pearl Harbor.

McManis: I don't think those are the same situations; there are different ingredients in all three. The world has changed dramatically since Pearl Harbor. It is interesting academically, perhaps, to look at these situations and try to understand the way human beings work, but to draw heavy lessons from very early crises, I think, can lead you down the wrong path. Perhaps that's true even for the Yom Kippur War in 1973 and other fairly recent events. We are moving so far and so fast. You don't want to lose sight of that.

Oettinger: Still, our hindsight is better than our foresight. Without belaboring the surprise issue, how often in a sizable national establishment — intelligence, media, academic, etc. — do people, prior to some event, point in several directions; yet they never have the conviction to carry their perceptions forward. In retrospect they say "Gee, I had it!" But where were they at the time? Perhaps at the time they were not persuaded that the weight of the evidence was sufficient, so they decided to wait a while. But still their files are there and sooner or later they will say, "I called that shot." It is a very delicate point to do that kind of post-mortem as to whether an event was in fact foreseen and effort was made to carry the word. I think the injunction is, "Thou shalt, if at all convinced, push the evidence forward." That seems to me an important injunction.

McManis: Yes. It is like an Amway motto: "Dare to Warn." In essence we have to get that motto to our analysts, and that is a hard thing to do.

*Princeton University Press, 1976