INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

Four Vital Issues in C^3I
Charles A. Zraket

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

Four Vital Issues in C^3I

Charles A. Zraket

Charles Zraket is President and Chief Executive Officer of The MITRE Corporation, a not-for-profit organization engaged in system engineering and research for military and civilian departments of the U.S. government, for state and local agencies, and for foreign governmental agencies. He joined MITRE when the corporation was formed in 1958, holding increasingly responsible technical management positions and then becoming Senior Vice President, Technical Operations, and later Executive Vice President and Trustee, before being named MITRE's President in 1986. Previously, he served as a group leader at the MIT Lincoln Laboratories Digital Computer Division. Mr. Zraket is a consultant to the Defense Science Board; a member of the Board of Advisors of Harvard's Center for Science and International Affairs and Chairman of the Advisory Committee for the Science, Technology, and Public Policy Program; a member of Stanford University's Center for Arms Control and International Security; and a member of the Committee on International Security Studies, American Academy of Arts and Sciences. He has published numerous papers and reports on strategic and tactical defense systems, C^3I, and other topics, including the 1987 book Managing Nuclear Operations, *which he co-edited with Ashton B. Carter and John D. Steinbruner.*

McLaughlin: Our speaker today is Charles Zraket, President of The MITRE Corporation. You all have the biography in your packet, so as usual we will skip the introduction details and ask Charlie to proceed. He figures that he has about 45 minutes of remarks. Are you interruptible as we go?

Zraket: Yes, please interrupt me at any time if there's anything that I say that requires some clarification or whatever. Let's be very informal.

McLaughlin: Let me remind you that MITRE over the years has been sort of an "angel" of these seminars: making transcriptions and production of the transcripts possible. So we feel indebted to Charlie and his predecessor, Bob Everett, and his colleagues out there in Bedford, who make this work possible. So, with no other introductions, the floor is yours and everyone should feel free to intervene.

Zraket: Thanks, John. As you probably know, my original talk was going to be on software and C^3I, but I decided last week that for this particular group I would like to take a broader look at C^3I. I will say some things about software, because it is a very important issue in future C^3I systems, but I thought it would be more worthwhile to let you know what's on my mind in terms of what I think the vital issues are in C^3I currently and for the foreseeable future.

Let me first enumerate five items that characterize the environment in which I think the C^3I systems have to operate now and over the next 10 or 20 years. My conception of C^3I is quite broad. I encompass in it the functions of planning or learning of military systems, the recognition function, the function of sensing information, the functions of understanding and assessing what's going on, and the action function — executing actions either with

weapons or other means. In that context C^3I has a lot to contend with in the coming years.

First, I'm sure you're familiar with the fact that we have a number of arms control discussions going on today: the Strategic Arms Reduction Talks (START), conventional arms reduction talks, and others. Those are going to create a number of adaptations and changes in our C^3I systems which I'll talk about.

Second, the major changes going on in the Soviet Union, with respect to the so-called "new thinking" that Gorbachev has initiated, are certainly going to change the parameters in the Cold War in many ways and put more emphasis on certain things in our C^3I posture, especially in the intelligence and recognition functions, that I'd like to talk about. Part of the motivation for the restructuring of Soviet economic society is that they recognize that they cannot keep up with us technologically with respect to the kinds of C^3I and weapons systems that our technology can now produce. I'll say something about that. They recognize that they've got to build their technological and productive infrastructure in such a way that they can develop and make these new kinds of very smart systems. So at least the Soviet military is in favor of *perestroika* in that it may help to restructure the Soviet military forces so that they can, in fact, compete with the rest of the world.

Third, if you take a longer-term look at the kinds of military threats that we will be facing in the future, they include stealthy vehicles — aircraft, missiles; much more electronic warfare than we have today; mobile weapons; what we call relocatable targets — targets that can move from one place to another with some preparation; and very smart air-to-surface and air-to-air missiles. For example, the French are already working on the next generation Exocet missile, which will be sold to many countries, and so those kinds of missiles are proliferating. I'm talking here not just about the Soviet Union, but worldwide.

Fourth, there have been some estimates that within the next 20 or 30 years, anywhere from 10 to 30 more countries will have nuclear weapons. Many of them will have the delivery vehicles for these weapons, whether they be ICBMs (intercontinental ballistic missiles) or cruise missiles. Many of them will have diesel submarines, naval mining capabilities, and chemical warfare, which is proliferated fairly widely.

Fifth, you have probably noticed the large numbers of so-called low intensity conflicts that exist around the world today, whether they be something in the Persian Gulf or some of these small wars that have been going on.

The reason for mentioning this kind of environment is that all of this affects not only the kind of military force structure one needs, but also the kind of C^3I one needs. For example, if we are successful in signing a START treaty and reducing strategic nuclear warheads by 50 percent, the command and control of the remaining 50 percent becomes even more important than it was. With tens of thousands of weapons one can afford to be somewhat inefficient, for example. So given that kind of environment, I wanted to discuss with you four specific vital issues that have impact on C^3I and are going to require adaptations in our C^3I systems.

First is the command and control of nuclear weapons. Here I want to put the emphasis on the command and control of these weapons from the viewpoints of readiness, safety, and security. Given proliferation of nuclear weapons, even if we reduce the size of the Soviet and U.S. arsenals greatly, we're still going to have a lot of nuclear weapons left. More and more countries are going to have them and will have them on more and more vehicles — not only ICBMs and aircraft, but also ships and submarines. So how we can improve the safety and security of these weapons during peacetime is going to be an important issue.

Second, I'd like to talk about the recognition function and worldwide intelligence capabilities, because as one couples military needs for intelligence with terrorism and drug running, and most of all, with the verification capabilities required for all of the arms control treaties that we hope we will sign, then intelligence needs become paramount. Our requirements for intelligence and our national technical means for verifying arms control treaties and knowing what's going on around the world at all times are going to increase greatly. That is probably going to have the most severe impact on C^3I, the I part of C^3I, the intelligence part, the recognition part. I'd like to say something about the collection of information and its processing and distribution and fusion, because with lots of different kinds of data coming from lots of different sources, then how that data is fused to arrive at coherent, accurate pictures is critical. The other major requirement is that all of this has to be done in real time or near-real time. It's not a situation where one can collect the data and find out days or weeks or months later what happened. One has to find out pretty much in near-real time what's going on.

The third area has to do with non-nuclear, or conventional, military capabilities. These are usually characterized by the so-called air-land battle, or the air-sea battle. Given the kinds of military threats I talked about earlier, the command and control systems for the air-land battle and the air-sea battle are going to have to change significantly, both in their recognition and sensing functions and in their action functions to operate in much closer to real time. This is also true, by the way, in the so-called low intensity conflicts, where one is going to need special kinds of sensing systems and coordination mechanisms. You can see the severity of some of these requirements when you look at even a simple operation like Grenada, which we ran and couldn't coordinate very well, even the communications.

Finally, if there's time I'll say a little bit about software. The reason software is becoming more and more important is, as these systems become more and more automated and depend more and more on computers for their operation, they become much more software intensive. Our ability to develop and deploy and test reliable software for these systems is going to become increasingly important.

Those of you who followed the debates on the Strategic Defense Initiative (SDI) have probably noticed that the software for the system is always brought up as a major limiting factor, because in many respects the hypothesized SDI is pretty much a completely automated system, depending almost completely on software. It's important when one talks about the software problem that one understands it isn't just the problem of coding programs for machines and checking them out. The thing that makes the SDI problem very, very difficult is not the software problem per se — writing code and testing it, it's the great uncertainties that exist in our engineering knowledge of the threat that the system has to fight against and our engineering knowledge of the performance of the sensors and the weapons that we're going to build. Since it may take 10 to 20 years to develop, build, and test many of these sensors or weapons, it's very difficult for us today to anticipate what the engineering performance of these systems is going to be and embody that in software that is very reliable. That's the position you're in with many of these automated systems and these automated C^3I systems: you have to anticipate what the engineering performance of these elements of a military system will be, so that you can embody it in the software code, and then when you find out more, you have to be able to maintain and change that code. So these are the kinds of issues that we at MITRE, for example, are facing all the time in helping the Defense Department to plan and develop and build C^3I systems.

Let me take the first one of the four issues that I wanted to try to cover this afternoon. That's the command and control of nuclear weapons. The problem today, of course, is that when we authorize the use of nuclear weapons, we send out something called an "emergency action message" (EAM), which authenticates the fact that the President has released these weapons, and we send that out to the weapons themselves. Some of our weapons, especially those that are deployed overseas, in addition to this authentication message, have what we call a "permissive action link" (PAL). It's a code. It's like a combination electronic lock on the weapon. One has to send the unlock code to the site in order to be able to use that weapon.

Today, to generate these messages, to send them to the weapons sites, to get all the approvals that are needed along the way, is a time-consuming process. That conflicts with the need for readiness so that if, in fact, these messages have to be sent out, they can be sent out rapidly. The systems aren't very reliable. People who have to unlock the weapons have a laborious processes of using codebooks to match up what they're being sent against the code in the weapon. Sometimes they don't have data links or computers and they have to send it all by voice in a prolonged phonetic transmission of voice messages. It makes for systems which aren't very safe and aren't very secure.

For modern technology, it's not very demanding; things that are being created every day today are very reliable, secure, digital data links, microprocessors, and public key encryption systems. One can embed these into what we call an end-to-end distribution system, where the authentication and the PAL codes are all built into the software code in the computer. It's all done automatically after first, the person authorizing the message checks it all out before it's sent, and second, the person way at the other end of the line receiving the message checks it all out before he acts. So it is possible, with modern computer and communications technology, to build computer and communication networks that will make this process much more secure and safe.

Why is that important? It's important that if we do, in fact, have a secure and safe system to do this, the people who have military responsibility for these weapons are going to be much amenable then to putting electronic codes on the weapons so that it would be impossible to have unauthorized use of these

weapons. That's the end objective: to be able to lock up these weapons, especially, for example, weapons that may be on ships that have dual missions. With the kinds of terrorism going on one doesn't want to have ships go into ports around the world with these nuclear weapons without being assured that they are locked up in such a way that an unauthorized person can't use them. At the same time, the system that locks them up must be safe and secure enough in terms of its readiness that the people who are in charge of the weapons feel confident that they really can control them when they have to.

So that's the trade-off. I only bring that point up because although we need modern computer and communications and software technology to achieve this objective, it's not a very demanding technological problem. The problem is very much a demanding operational one and a system problem to ensure that whatever nuclear weapons we, or anybody else, deploy worldwide we can keep safe and secure. I might point out that most of the nations that currently have nuclear weapons — the Soviet Union, the French, the English, the Chinese — feel the same way. I think everybody feels the need for this kind of capability. The fact is that the Soviets copied our original PAL devices that we started deploying back in the late 1950s and 1960s. It was a technology we essentially leaked to them — how to do it. That's one vital issue that you don't see discussed too much, but is something I think that everybody who is in the business is very much concerned with, given the proliferation of nuclear weapons that's going on today and will go on in the next 10 or 20 years throughout the world.

Student: I'm curious as to what exactly your ultimate point is as far as whether we should leak this, or just give it or sell it to other nuclear powers, or are you saying that it's time to modernize our forces?

Zraket: It's time to modernize our system. The Defense Department already has development work going on in this area, so this is something that's not new to the Defense Department. The idea is to develop it, test it, and deploy it. I think once we do that and show that it can be done, other nations will pick it up.

Student: I have a couple of questions. I'm curious as to why we would modernize because, as I understand it, virtually every nuke outside of Navy sea-based nukes has a PAL of some sort incorporated in it. The other day I listened to General Galvin* talk about one of the worst possibilities, a blitzkrieg attack by the Soviets in Central Europe, and how he would call for the use of a nuclear weapon after approximately 10 to 14 days. That's what he felt that he had. His words were, "I would send a signal to stop the war by the use of a nuclear weapon and it would be a land-based nuclear weapon." Well, that gives us 10 to 14 days, so I'm curious in these times of budget constraint that we're facing, because the weapons are safe now, at least from a layman's point of view. It might be time consuming, it might have a reduced readiness, but if you have 10 to 14 days in probably the worst scenario going, why spend the money?

Zraket: For a number of reasons. One is we don't have selective release of weapons, so you either release them all or you don't. Two, you do have weapons on ships around the world, where you kind of blithely said we have a PAL on every weapon but those on ships, but ships are very important. We have hundreds of ships around the world. Many nations are going to start having nuclear weapons and it would set a pretty good example if, as more and more nations have weapons, they put locks on them.

We haven't had a terrorist attack against some of the weapons sites but it's not out of the question. Such attacks could take place, especially as weapons are more and more proliferated around the world. So I don't think we could take great comfort in the fact that because only we and the Soviet Union have nuclear weapons today and we have taken pretty good care of keeping them that that's the situation that's going to exist for the next 50 years.

The fact of the matter is that the system is not very selective today. It is time consuming. You might say we have 10 or 14 days, but what if on the fourteenth day General Galvin decides he wants to release these weapons and finds it may take three or four hours instead of 10 minutes to unlock them? He may worry about that kind of problem.

Student: Then we come to the question of when you lock or unlock during your mobilization. You don't have much time during a blitzkrieg, which is obviously an extreme scenario.

Zraket: If you unlock them ahead of time and all of a sudden they get overrun, there are times you may want to wait a little bit more. All I'm pointing out is that for a relatively trivial amount of money compared to the cost and size of the forces, modernizing a system like this to make it more safe and secure and responsive at the same time seems to me like a pretty good idea. Especially if you start talking about more and more proliferation of weapons and the fact

*General John Galvin, USA, SACEUR.

that one would like selective release mechanisms so that if, God forbid, you wanted to use one or two of them, you didn't have to release a thousand in order to be able to do that. Using one or two nuclear weapons could be a catastrophe, but compared to unlocking a thousand such weapons, there's a big difference.

Student: When you talk about a lack of capability for selective release, are you saying the EAM structure does not currently admit the selective release of nuclear weapons by category or by individual identification?

Zraket: I'm talking electronically. There are selective releases in terms of the orders, you know, "You're authorized to use four of these for this purpose," so there's selective release that way, but if you have 200 weapons in your inventory, you might have to unlock all 200 in order to use four.

Student: Why is that?

Zraket: Because of the deficiencies in the electronic system that locks these up today.

Student: Some of these could very well be like artillery shells. This is a technical problem.

Zraket: It's a technical problem. I'm solving a technical problem, not an operational problem.

Student: Unlocking means just that they are now operative to be fired?

Zraket: Unlocking means, imagine that you have a safety lock and you have the combination to take the safety lock off so that the weapon is available for use. That's what we mean by unlocking.

Student: Unlocking is a manual process?

Zraket: Right.

Student: And some of the codes go by voice systems?

Zraket: Some of them might be sent down by voice, but the actual physical process of unlocking them is manual.

Student: Weapon by weapon?

Zraket: Right.

Student: Then why is there a technical limitation on which weapons you choose not to unlock and those that you choose to unlock?

McLaughlin: Because you've issued the key that works on all the ones in that particular armory.

Student: But why can't one simply decline to unlock x number of them? Why is that a technical problem?

Zraket: Because once the key is released, anybody can unlock all of them.

Student: Okay.

Student: There's a corollary here that if you have a compromise, you're faced with the problem of, do you call all the submarines back, do you do this ... ?

Student: So you have to assume that everything that can be unlocked, having received this code, will be unlocked.

Zraket: Right. What I'm talking about is a technical problem that has a technical solution. It involves using more reliable digital data links, and computers and software to do the mechanical part of the job more accurately and faster. Everybody gains. You gain from an operational viewpoint in that you have a more responsive system. You also gain in that you have a safer and more secure system.

Student: Mr. Zraket, by calling this one of your four major issues, you seem to imply that there is some controversy or some reason why this is not proceeding at, perhaps, the pace that you feel it should. Is there a problem with money or politics? One would think that the safety of nuclear weapons would be a sine qua non. You know, you go a hundred percent and then some.

Zraket: I think you heard what I would call the archetypical reaction of most people in the Defense Department to this idea. "Why spend the money? Everything's working fine now. We don't have to do it. It works great. We don't need it." Are you a naval officer, by the way? Yes? I figured as much.

You take the Air Force, you square it and that's the Navy. I work a lot with the Navy, I'm an overseer of the Center for Naval Analyses, and to their credit, they're really looking at this problem very seriously now. They're performing some very honest intellectual studies on what the trade-offs are and my guess is they'll come up with some good answers. The Navy moves slowly on some of these things but once they decide to do something, they really do it very well. Whether they'll end up putting it on ships and subs I don't know, but they're looking at the problem.

There's a big wall that one has to overcome in implementing something like this. So it is a vital issue. The importance of the issue is very high compared to the technological and economic aspects of it. That's why I bring it up.

Student: What kind of cost are we talking about to implement a system?

Zraket: The computer software costs are trivial. You're talking about microprocessors, minicomputers, and putting these in various control centers that control this process at the various commands, whether it's CINCLANT, or CINCPAC, or SAC, or whatever.

The survivable digital data links, of course, are something that one's going to need anyway for a lot of other reasons. The idea is to ride on the worldwide survivable digital data links we're building already, satellite links or fiber optic links, or HF links, or whatever. So I don't think the costs are very high. Certainly the worldwide links in and of themselves can be fairly expensive, but we're going to have them for a lot of other reasons and the bandwidth you need to do this is fairly trivial. In the same way that we use the Milstar system, for example, to send out EAMs today, you send this kind of stuff over that link just as easily. What you need is the computers and software on both ends of the process.

I'm not enough of a weapons expert to know what you actually have to do to the warheads. Sandia has been studying that. That probably has a retrofit cost associated with it and I really don't know what it is. I would guess, in terms of the mechanics of the process, that's probably the most difficult thing to do: just to go back and fix up all the warheads so that all this can be done reliably and well. But I think it would be a good thing to do, as I said, because if we can set the example everybody else might follow us. I've got to admit the Navy's been very thoughtful about this subject the last year or so.

Okay, let's go on to intelligence. Let me say first that here, again, the technological advances in our ability to collect information worldwide have been very dramatic in terms of the kinds of sensors we can deploy in space and around the world. They cover the whole electromagnetic spectrum from microwave active radar systems to passive systems using visible and infrared and ultraviolet spectra. We can get all kinds of data on anything you want to think about. We not only have air-based radar such as the AWACS (the Airborne Warning and Control System) that can track aircraft, but we're also building something called Joint STARS (the Joint Surveillance Target Attack Radar System), which is an air-based radar that can see ground targets. So in terms of sensor satellites from space, and sensor systems in aircraft, and sensor systems on the ground, we have a really dramatic capability to see everything that moves, and everything that stands still, with many of our synthetic aperture radars, for example. So we have a very dramatic technical capability for sensing, and in the future probably our defense budgets will be more important in determining how much of this we deploy than any technological limits that we have.

There's going to be a tremendous emphasis on deploying these systems and giving them much greater what we call survivability and robustness, especially for the space-based C^3I systems. One of the problems from which the United States suffers in this respect is that, as evidenced by the Challenger accident to the shuttle, we do not have a very robust capability to launch our satellites into space. So for the past few years we've suffered in our ability to deploy satellites that we have designed and built. The Soviets are much more robust than we are in this respect. They've demonstrated time and time again that they can put up multiple satellites on a daily basis with their launch capabilities.

Secondly, our satellites in space need to be protected against anti-satellite weapons, and that means spending money to harden them, to make them maneuverable, to make them less susceptible to jamming, and so forth. So, the second point is that all of this technology that I just cycled through means that when we deploy it, it's going to be more expensive because of these factors of making it more survivable and robust.

McLaughlin: Charlie, let me ask you a question. Someone a few years ago made the observation that the defense field is the only area in the entire electronics industry where things get continually more expensive instead of continually more cheap.

Zraket: There is in fact a technological inflation that's taking place, or has taken place, in defense systems, in the same way it has taken place in commercial systems. This is a true technological inflation, and there have been studies that have documented it. There has been a study made of naval air systems over the past 15 years, and the so-called technological inflation has been something like 4 or 5 percent a year, which means the cost of the systems has doubled, leaving out economic inflation. What this means today is that when you go into your Plymouth or your Chrysler car and you look at all the technological features in it, and compare it to the Plymouth you bought in 1950, there's a difference of night and day.

The same thing has happened in our military aviation. The avionics now is a much greater percentage of the cost of that aircraft than it was 20 years ago. Its capabilities are much higher. I'm sure you've seen some of these diagrams that take the curves of

the cost of military aviation. You take them out long enough and we'll end up buying one airplane with the budget that we have. So, the fact is that on a per unit basis we have had a 4 to 5 percent increase in complexity per year, on the average, on most of the stuff we're buying. If that trend continues into the future, it means we're going to be able to buy fewer and fewer units for a given budget than we can today.

McLaughlin: Again, if you look at the commercial applications, the Boeing 747 that rolls out early next week or whatever is a considerably more sophisticated plane than one made 20 years ago. Of course, the multiplier is nowhere near what it is in the military sector as far as I can tell. One side of the argument is it's a lack of effective competition because all these systems are so expensive with one contractor, two contractors, or the consortia. It's not like "Gee, the 386 computer I'm getting next week, or whatever, has the same price as the PC I got a few years ago except it's 10 times more effective." It's a 50 times more effective machine. It seems that I frequently get the answer, "Well, it's technologically a lot more complex." Well, that's true of a lot of other sectors but the prices still come down, which we have not seen in the defense arena for a long time.

Zraket: They are coming down in certain areas. In fact, I was just going to point out that one of the trends that has occurred because of this is in the fields of processing and fusion of information in the intelligence business, leaving out the sensors for the moment, which are unique to the Defense Department. There's no question that the Defense Department is pioneering in the sensing technology, because they have the requirement for national technical means of warning, for verification of treaties, for reconnaissance and surveillance and target acquisition, and what have you. But what's been happening in the processing and the distribution and the fusion of data is that we've been going more and more to commercial systems. We've undertaken efforts in the so-called open systems architecture. For those of you who follow what's going on in the electronics business, this has happened even with the very large manufacturers — IBM, DEC, AT&T, and so forth. We are defining standards so that one can assemble large-scale processing and distribution systems in such a way that you end up with what's called an open systems architecture. You can take computers and workstations and communication systems from different manufacturers and put them all together into the system of your choice.

In the case here, the Defense Department, where the data is coming from multiple sources, and has different levels of security associated with it, that becomes a little more difficult than when you're working in the commercial world and you don't have a security problem other than single level security, if you will. So people have been working on taking commercial workstations of the kind that Sun and Apollo and others are making and adding software to them to have what are called "compartmented workstations." These workstations are able to take in data from many different sources, with different levels of security depending on what the workstation is designed to accept or not accept, and they allow many of these intelligence processing distribution centers to take in data from many sources, process the information, fuse it, and distribute it according to whatever security levels have been set up.

The National Security Agency has been working on networking techniques. Those of you who are in the business may have heard of blacker type systems that are designed to control all the access of people to data that's going to and from these systems. It's a very complex technical effort that's going on, but it's an attempt at least in the processing and distribution part of it to depend on the commercial base of large-scale economies of scale, using standard workstations, and standard computers, and standard displays, and standard networks, and bringing in the DOD software that will add the security function along with black boxes that will restrict access to many of these processors, and be able to build networks into them. That's another significant trend that's going on in the department. It's just started in the last few years. The Defense Intelligence Agency, the National Security Agency, the CIA, and most of the intelligence agencies are going in this direction of not each building their own tailor-made hardware and systems but going to these open system architecture approaches.

How you solve the technical inflation problem in avionics and in sensor systems is a real problem for the Defense Department. They don't have a conceptual solution to the kind of problem you're bringing up. The advanced tactical fighter (ATF), for example, which the Air Force is developing, has a proposed avionics suite that's going to have literally millions of lines of software code in it. That's as complicated and as large as most of the ground-based systems we've built in the past. This is going to be a very smart airplane.

The B-1 is an example, of course, where we had a failure in the avionics system. If you've all read the

newspapers, you know that the B-1 had a very complicated avionics suite, both offensive and defensive. It's a very good airplane, contrary to what you might have read, as an airplane. But the fact is that the software code and the electronic warfare parts of that did not meet the specifications that were set down. It's a very complex job whose complexity was underestimated. Now they have to go back and try to get the money to fix the system and retrofit it.

Student: You've mentioned technological solutions, the technology-driven approach to these problems, but wouldn't there have to be a nontechnological decision, especially when you think about something like the ATF, such as: this is too complicated, we'd rather have an airplane with half as many lines of code in it, or wherever the price tag is. So how do you address the larger question of the costs?

Zraket: Don't misunderstand, I wasn't advocating that it should be that complex, I'm just telling you what the specifications for it are stating.

Student: How would you address the problem of drawing that line? I was looking at your other points and it seems they were all going to have, once again, software and C^3I for conventional operations. Again, this is heavily technology driven, but clearly you can push the limit of that. How do you decide?

Zraket: Actually, I could suggest a process solution to this. I can't suggest an answer because it's a very complex problem. If you look at the avionics suites that are going into advanced aircraft today or into satellite systems, it is true that is what's been happening. Satellites are a very good example of that, where we have ended up with 10,000-pound satellites with very complex electronics in them. There has been a move, the so-called Lightsat program, which is partly spearheaded by DARPA (Defense Advanced Research Projects Agency), that this is crazy. Let's stop building these huge 10- and 15- and 20,000-pound satellites that are so complex. Let's see if we can partition the functions that we have to build into these things and build smaller, simpler satellites that we could turn out as though we were using cookie cutters. This is certainly true in communications. There's no reason why you couldn't put up a couple of hundred of small, simple communications satellites in a packet-switched network and get the kind of capability you might get by putting everything in one big satellite and one big high-speed switch, for example. So people are talking about techniques to try to understand the functions better, partition those functions into smaller, simpler pieces that you can then build in a very simple way, turn them all out, and deploy them that way.

What the analog is to the aircraft case, I don't know. I do know, though, that in designing many of these avionics suites, one of the approaches that has been taken is to look on each aircraft as a kind of self-contained, total C^3I system that doesn't have to depend on anything else in the world other than that one aircraft. It would be completely self-contained and self-sufficient, so that when that pilot goes out with that airplane, his dependence on the ground, or on getting information from anybody else is minimized as much as possible. That's the whole idea that was sent out. I don't know whether that's really a good idea or not. You can argue one way or the other. Maybe it's simpler if they made the avionics and the airplane somewhat simpler and depended on some more coordinated scheme between the plane and other airplanes and air and ground and so forth. I haven't thought enough about it because we're not in the avionics business. I can't give you a good substantive analog there, but certainly this kind of approach is driving the unit costs of these things up to the point where they may not be affordable. So one ought to be taking different kinds of approaches to this.

I think John hit on a good problem of how you break the back of this technological inflation that's been going on in most military systems. It's a very severe problem and needs a lot of attention. Again, the Navy seems to be leading the effort here; it was their study that I quoted. They're the ones who are actually studying the problem and trying to decide whether or not they have too many different kinds of platforms, whether they're too complex, or whether they can do the job a better way. So people are certainly aware of it.

McLaughlin: Let me make one other observation. ATF, I think, represents about three different fields of technological dilemma. How do you build the next generation of fighter planes? You can't make it any faster because we've already made faster fighter planes and the performance is degraded because they go much faster than the pilot can handle, even given all the electronic support, and so forth. So we build slower ones than we used to build. I mean, we peaked out in speed with SR-71s. You can't build them more maneuverable because the pilot cannot handle the G forces with greater maneuverability. Today the plane is more maneuverable than the pilot. So, the next generation aircraft will not be any faster or any more maneuverable than what you have out there now because the pilot can't cope.

Student: Why do you need a pilot? Just drive it from the ground.

McLaughlin: Well, that's one of the issues. Going back to Charlie's question about what you put on to the platform, in so many of these situations you assume the platform is being operated under the control of another platform, whether a Hawkeye or an AWACS, and you replicate everything on the individual fighter plane that you also have on all those control platforms.

Zraket: The problem is being recognized. One other example I'd give is that some of you may remember the LHX (Light Helicopter, Experimental), the Army's new attack helicopter. They proposed a machine a couple of years ago that makes the ATF look like a simple thing. My predecessor, Bob Everett, chaired the Defense Science Board committee that looked at that and Bob was honest enough to say "This is absolutely ridiculous. You could never build this thing that they're talking about." They cancelled the program. The Army did not like it. That program has been in a lot of trouble for the last two years. They're having trouble resurrecting it.

Snyder: This is a question that maybe you'll cover in the software thing, but in the discussion we had a minute ago about the cost and the weight of the increased complex software, is there not another problem here? In a system where a million lines of code represent a million decisions, a million doors opening and closing, isn't there concern on the part of some people that we don't know what's in the software anymore? It's so complex that we, or the drivers, are not sure what decisions have been invented in there. Are we reaching the point where there is some concern about that?

Zraket: There is a lot of concern about that, although if there's one field that I know first-hand, it's software, because at least most of the technical work I've done in this world has been in computer design and software design. It is possible to design software rigorously and to test it and verify it, but it's expensive. The problem is that people relegate the design and development and test of the software to an afterthought and it's become a garbage pail. When people design systems they say, "I'll put all that in the software." And then these problems end up with the teams designing and coding the software and testing it.

I gave a talk Monday at an AFCEA (Armed Forces Communications and Electronics Association) conference that was made up of mostly DOD and industry officials, and pointed out that it was absolutely disgraceful, the amount of money that DOD was spending on software research and software engineering tools and industry incentives to put good trained people into software. Today we spend $30 billion a year directly; that's 10 percent of the DOD budget, and it goes into the development, operations, and maintenance of software on computers. The cardinal rule in any enterprise is, you spend about 10 percent of your total expenditures on research and development to make sure that you're furthering that art and doing it right. That means we should be spending about $3 billion a year on software research, and on software engineering tools to help us build better software. Well, we're spending about $100 million or $200 million a year and it's fragmented. It's the kind of research that's sent out in hundred-thousand-dollar bites to universities as hobby shops.

So DOD is not taking the problem very seriously. It really is a disgrace. Here's something that's absolutely essential to everything they're doing in developing weapons systems, and they don't pay any attention to it. They're assuming that somehow, magically, the commercial database in this area is going to do it for them. It is similar with VHSIC (very high-speed integrated circuits). It's turning out now that all of the defense contractors who worked on the VHSIC program are giving up on it because commercial electronics is driving them right out of business. They don't have the applications for the VHSIC to make it worthwhile for them to invest in it. So the technology base that DOD needs in electronics and software does not exist today in industry. DOD is almost completely dependent on what the commercial market is supporting, and the commercial market does not do the kinds of things DOD needs in their systems. So the infrastructure for these complex, high-tech systems that we're developing and building in electronics and software does not exist in the industries that support them. Now, I'm not the only person saying that. You go talk to any of the defense contractors and they'll tell you that in spades. It really is a disgrace! The Army will sit down and they'll design this LHX and they've got a set of requirements that will take the next 30 years to implement in terms of our knowhow in electronics and software and sensors, and want to put it all in a helicopter. You just can't do it. They were shocked when somebody told them that.

Let's talk about another subject — the air-land battle C^3I. Now here's a case where the payoff can be very, very high if we develop the so-called force multiplier capabilities that would increase the force

effectiveness. The idea is to take, for example, the air-land capabilities we have and try to build an all-weather capability in them as well as a day-night capability. That's especially important in Europe, where the weather is always bad.

The second thing one wants to do is try to build as long a range of standoff as possible for the manned systems that are carrying air-to-surface and surface-to-surface missiles so that one can increase the survivability of the manned systems. The third is to build as autonomous a delivery system as possible so that you leave people out of it as much as you can. And fourth, you build multiple kills per pass of a weapon so that if you send a weapon out against a set of targets, it has enough ordnance in it that it can make multiple kills.

What those kind of capabilities do for you, of course, is that they greatly reduce the overall firing rate that you need in the system. In the case of aircraft, they greatly reduce the number of sorties you have to fly and the number of bombs per target kill goes way down.

To achieve these kinds of capabilities, one needs what I talked about earlier: real-time reconnaissance, surveillance, and target acquisition capabilities. That's the purpose of the two systems I mentioned earlier — AWACS and Joint STARS. These are air-based surveillance systems that can see air targets and ground targets in real time, and give the targeting information to the weapons. These are smart weapons that have sensors in their warheads that can sense the target when they get there; either, say, it's an IR (infrared) sensor or in some cases such as the Pershing missile, it has a picture of the target that it's going after and when it arrives there it compares the two and then if that's the right one, that's the kill. It's basically mutual pinpoint accuracy. So this is a case, I think, where by distributing all of the functions among sensors and smart weapons, and standoff command and control platforms, one can achieve very high productivity, maybe increase the productivity in these systems by factors of 2 and 10.

So that's a big thrust today in much of the research and development that's going on in the Air Force and Army to increase the efficiency and effectiveness of their ground-based and air-based weapons. The Navy is going through a similar process. The Navy is especially concerned about the fact that weapons such as the Exocet (the sea-skimming cruise missiles) or other kinds of air-to-surface missiles or surface-to-surface missiles put all of their ships at risk. So they have a very strong need to be able to field sensor systems that can first sense the delivery vehicle itself, whether it be a ship or an aircraft, what they call over-the-horizon — far enough away that they can maybe intercept and destroy the delivery vehicle. Or if, in fact, they don't do that, that they can sense the missiles coming in and fire weapons against them before they get to the ship. So they have a lot of research and development going on in new sensing systems, new communications systems, and a concept that they call cooperative engagements, so that the ships in a battle group would be netted together with a high-bandwidth, anti-jam communication link. Through cooperative engagements and exchanging sensing information and weapons assignment information, they could optimize their defense of the whole battle group. So that's a very important part of the Navy efforts that are going on today.

So both in the case of the air-land battle and in the case of the air-sea battle C^3I, in the form of new sensing systems, both air-based and ground-based, and new communications systems and new sensing systems in the weapons themselves, there's a revolution going on essentially to increase the survivability of those forces and to increase their effectiveness in terms of the number of sorties they have to fly, and the firing rates they have to have, and so on. So that's another answer to the question posed earlier, that in fact one could envision using these kinds of technologies to get factors of up to 10 improvement in the efficiency of the systems.

Student: Do you foresee the use of blimps in any of this?

Zraket: That's one of the options being looked at as a platform for sensors. The Navy's been doing most of the work in that area because if you want to see low-observable targets at far distances, you have to get up there and look for them from the air.

McLaughlin: It will revitalize Lakehurst, New Jersey. I think they still have those blimp hangars there.

Student: In some of the other sessions we talked about military education. Do you think that the level of technical education of basically the lower ranks in the military is going to keep up, and that we'll be able to support these kinds of systems effectively? Or is that going to be a problem?

Zraket: I don't know firsthand. The people I talk to in the business say that they probably have the smartest group of soldiers and sailors that we've ever had. They undergo a lot of good training programs.

One thing I didn't mention is that in the intelligence area, at least, we're now building automated systems to help in the training of intelligence people both in terms of teaching them languages and teaching them to recognize different kinds of signals, and so forth. There are automated and semi-automated systems now being built to train people to be intelligence technicians, and the same kinds of things are going on terms of the operational people themselves.

I know in a lot of the exercises that have gone on, this is an extremely important matter because in one particular overall system I'm not free to identify, the learning curve over a two-year period of exercising that system in realistic exercises, and training the operators without changing the design of the system at all, went from something like 40 or 50 percent effectiveness to 90 percent. This involved, for example, training operators in aircraft to learn how to use satellite terminals to get information in and out of the airplane and things like that.

That kind of training is absolutely essential. We probably don't spend as much money as we should in realistic exercises. Many of the operational commands have very limited budgets for training and exercising their people. That's one thing the Soviets do very well. They're exercising all the time. They have very set routines in how they do this, but they design a routine and they really perfect it.

McLaughlin: Charlie, under almost any of your four vital issues, and since the training question was asked, you mentioned getting some more productivity out of the conventional systems. Domestically, if we look at the 20- to 24-year-old age group, the labor force goes down between 1985 and 1995 by 19 percent. For years I've been talking with people from various services about what you do when there's a decline of 19 percent in the pool that you can pick from. I'm talking about the labor force in which you can't stretch the woman labor force much further, at least in the United States as compared to Spain or Japan. Do you see any of the services looking at C^3I, or electronics, as a means of combating this? For the people I talked to it's sort of like the 27th priority to worry about: where the bodies were coming from. Have you gotten any inkling along these lines?

Zraket: The only examples I can give are the kinds of automated systems I was talking about. The two that I'm aware of are the automated communications systems such as the mobile subscriber equipment that the Army is putting in all over the Army and some of the Air Force — TRI-TAC (Tri-Service Tactical Communications) and JTIDS (Joint Tactical Information Distribution System) equipment. The number of people that they need to operate and maintain these systems has gone way down. They are a real saver in people. The Army, for example, was able to eliminate something like 5,000 people in their communications maintenance groups because of the increased automation and the need not to have the tape tearers, and the higher reliability of these systems. Most of this modern electronic stuff is much more reliable than what we were getting before. In fact, if you go talk to a lot of the people in Europe, as I did, about how they like the JTIDS terminal and how reliable it is, they say "I don't know. I've never had to fix anything." This is very, very unusual for an airborne piece of equipment in an AWACS airplane.

So I think a lot of the automated electronics in sensors and communications and computers in the control centers are going to reduce the need for the lower-level technicians and operators who used to people many of these military systems. In fact, if you talk to the Air Force about the pilot of the future, they talk about him more as a chess person than a controller, if you will, or a flyer. He's somebody who's going to orchestrate lots of missiles and lots of capabilities through his symbiosis with these electronics more than he is going to be flying an airplane, trying to out-dodge the other guy. So I think there's some hope in that area that dependence, especially on the lower-level operators and technicians, is going to be greatly reduced in many of these systems. You certainly see it in the training. We've built three training systems for the intelligence community down at Goodfellow for training intelligence operators, and these things get the people through the system faster with fewer people. So, you know, it really works.

McLaughlin: Maybe I should let you get to software.

Zraket: I've already said most of the important things I wanted to say about the software. One of the buzzwords going around with respect to software is "artificial intelligence" (AI). What difference is that making in C^3I systems? It turns out that so-called artificial intelligence, or expert systems, is starting to be applied in military systems. In force application there have been some examples where decision aids are being employed, mostly in the planning area. We participated in one, a tactical air planner, where one can build a computer program that has the U.S. and the enemy orders of battle stored. The tactical planner can sit at the console and decide, given the mission he has, to attack a certain target, have the

computer help him select which aircraft from which base he ought to use against that target; what surface-to-air missile batteries he has to face in going there; and how he would overcome them. So a planner can sit there and go through maybe 10 or 15 different plans and compare them in a matter of an hour or two, whereas previously it might take him a whole day just to plan one mission and get it done. There have been tremendous increases in examples like that.

There's been a lot of work in helping to deliver and assess resources. The Army, for example, has built AI tools to help them in how they deploy their mobile subscriber equipment. For those of you who are unfamiliar with that, this is a set of communications switches that go along with the Army on the move, and they have to figure out the best place to deploy them and interconnect them and so forth. One can build automated tools to help them do that. One could also build tools, and this has been done with some of the Army forces in Europe, to help them to decide how to expend ammunition. One of the big problems that faces Army commanders is that they have a certain ammunition supply and they can't tell very easily what's going to happen over the longer term if they start using large amounts of it against certain targets. This program will play out the decisions for the commander and tell him very quickly what the net results of his firing rates are going to mean in terms of his ammunition supply and so forth.

So there's a whole set of decision aids such as that and the recent work uses neural networks to help people decide how to distribute control in a system and so forth. There's a lot of work going on in that area, I think, that holds promise to increase just the everyday logistics and planning and resource expenditure in many of these systems. And, again, that's going to help in reducing the need for low-level manpower.

All of this, of course, has to be manifested in software, and I don't want to be too technical in that area right now except to point out what I did earlier: the only solution to building reliable software is to have very rigorous designs of what it is one wants to do, designs that are mathematically consistent. One of the big mistakes that people who build large-scale software systems make is to get right into coding the program based on some seat-of-the-pants understanding of what it is they want to do. You really have to sit down and look on software design as a very precise mathematical problem and do a very rigorous design that's self-consistent and that you can understand. It must be self-consistent enough and partitioned enough that you can go back and in a mathematical way verify what it is you've coded to see that it's consistent with the specifications that you've designed.

We now have techniques to verify the specifications for the software, but we don't have techniques that can verify the actual code that gets translated from the specifications by either people or computer compilers into code. That's very, very difficult to do. To verify those programs, especially if they're very critical in terms of ensuring computer security, or if they're very important control mechanisms like controlling the modes that the satellite will operate in, you literally have to go in and go through the code step by step and verify it manually to ensure that it's reliable.

All that is a way of saying that this is a very labor-intensive activity. It's very highly skilled, expensive labor, and so it's a very expensive process. Most of the studies that have been done have shown that over the life cycle of highly sophisticated computer systems that are software intensive — it might be 10 or 15 or 20 years — the software accounts for 80 percent of the cost of the system. That's to design, generate, test the software, and modify and operate it. So it's a very expensive thing and one has to budget for it. So, let me stop there.

McLaughlin: Your timing was good. I'm sure everyone would like to join me in thanking Charlie. We all found it very useful.