Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Role of Intelligence Within C³I

Lincoln Faurer

Before his retirement, Lieutenant General Faurer was Director of the National Security Agency, and Chief, Central Security Service, Fort Meade, Maryland. General Faurer has had an extensive military career, including deputy chairman of the NATO Military Committee in Brussels, Belgium and Director, J-2, for the U.S. European Command in Vaihingen, Germany. He has worked several times for the Defense Intelligence Agency, most recently as Vice Director for Production. General Faurer is also the recipient of numerous decorations and awards, including the Distinguished Service Medal, the Defense Superior Service Medal with one oak leaf cluster, and the National Intelligence Medal of Achievement for his service to the national intelligence community.

I am delighted and honored to be here to discuss command, control, communications, and intelligence (C³I). I believe C³I is indispensable to the successful conduct of military confrontations. That C³I has become a central consideration in defense planning results from an attitude that has evolved over the last half-dozen years, and it represents important change.

Half a dozen years ago, C³I was in a gray area between operations and intelligence. Now, C³I is getting much more attention as policy and planning take place, including increased investment in C³I systems.

As you may imagine, given my position and background, I will focus on the intelligence aspect of C³I. What I hope to do is explore the options for supporting military commanders. Remember, there are several levels of military command. The support needed by a SACEUR (Supreme Allied Commander Europe — NATO), for example, is quite different from that needed by division commanders in Europe. My remarks will focus on the provision of timely, accurate intelligence tailored to the needs of the various commanders.

I have been in the intelligence business, or on the edges of it, for a little better than 20 years. Early in the '70s, I was an intelligence user as the J-2, or Chief of Intelligence, for U.S. Southern Command (SOUTHCOM) in Panama, with responsibility for Latin America. Later, I was in a similar post in Europe, again as a J-2 at U.S. European Command (EUCOM), with similar responsibility for the European theater. In between, during the mid-'70s when I was with the Defense Intelligence Agency (DIA), was responsible for all of the DIA's intelligence production. So I have been both a user and a producer of intelligence.

I also found that spending two years just prior to accepting my current position at NATO headquarter was a very profitable experience for understanding the intelligence user's needs. As the Deputy Chairman of the Military Committee, I studied the demands for intelligence placed on NATO's military structure. My focus today is derived from having been the Director of the National Security Agency (NSA) for the past four years.

So, what is the intelligence mission for the NSA? The Secretary of Defense is directed to serve the

President as our government's executive agent for three missions: the provision of signals intelligence, the provision of communications security, and the provision of computer security across our government structure. Those are in addition to the hat he wears as the Secretary of Defense. As the Director of NSA, I am charged to manage that executive agency responsibility for him. The NSA is responsible for collecting, processing, and disseminating signals intelligence (SIGINT) and the information attendant to that. Today we're going to concentrate on the defense establishment, a major customer of SIGINT, and specifically, that intelligence used for the conduct of military operations.

I take my general tasking priorities and standards for timeliness from William Casey, the Director of Central Intelligence (DCI), and his apparatus, as well as the committee that oversees intelligence requirements for the entire government community. For defense purposes, I take my specific guidance from the Secretary of Defense and from his military commanders for the establishment of hostilities-related tasking priorities and standards of timeliness. I will not dwell today on our other two missions, but may touch occasionally on communication security as it affects C^3I. However, as an agency, we do have to worry about that side of the coin.

While I am attempting principally to obtain SIGINT for others, I also am trying to protect our own signals, our communications, from exploitation by the other side. A reasonable extrapolation of this, which occurred within the last several months, was the assignment of a similar responsibility for computer security.

Underlying virtually all I will say, and essential for your understanding, is SIGINT fragility. Success in gathering signals intelligence requires an advantage over the other side. The other side must not know exactly how we gather intelligence or the extent to which we are able to exploit it. Stories that have come out about the World War II Enigma machines and the exploitation of Japanese communications illustrate this. Our success had to be a carefully protected secret in both instances to have survived the war and to have left us with that advantage over both enemies. Any disclosure or hints of capability could have provoked relatively easy changes by the other side, which would have denied us an enormous advantage.

The world has not changed that much since World War II, and our present advantages must be protected. They can be destroyed very easily by media references to intelligence successes. I regret that we see these as often as we do. That we listen is not secret. Anyone can imagine that "to listen" is our mission. What is important is that our successes be protected. I have made a point of asking senior people in the news media, managing editors and higher, to spend a few hours with us at the agency and to allow me to sensitize them to the problem of SIGINT fragility. Often I encounter a belief on their part that the United States is so capable that we must be able to divine what any target country is saying, doing, and transmitting. The media uses that image of our omnipotence as an excuse for being able to talk freely about success. But that image is ridiculous. We can't possibly do everything.

There are several operating principles for accomplishing our missions. NSA and the other elements of the U.S. SIGINT system function as a unified organization. We learned in World War II that we would be better served in the SIGINT area if there was consolidation. And so, after two or three false starts in the late 1940s and early 1950s, today's National Security Agency evolved with some responsibility for similar capabilities within each service. I'll touch on that in a moment.

Another principle is that our functions are centralized or decentralized as needs dictate. For example, technical tasking is centralized. The actual collection is decentralized. Our aim is to achieve the greatest possible responsiveness to the stated requirements at the least possible cost. There are all kinds of checks and balances in that equation. The Congress, among others, emphasizes minimum cost. All of the customers emphasize their requirements. We are the ones in the middle trying to find the balance between cost and requirements. We're designed to respond to the needs of authorized users, to make rapid and direct delivery of that information. That means in part that you want to give people what it is they must have, and yet you don't want to give unnecessary information to people, for security reasons: the simple "need to know" rule of thumb. For his own sake as well, you don't want to overburden the user with information he doesn't need. Finally, all of our operations are conducted in accordance with the law. That's not just a sort of gratuitous throwaway line, it really is considerably significant.

Despite the fears and suspicions of many sincere citizens, my agency conducts itself very, very carefully within the law for many good reasons. Aside from moral imperatives, we do it because the work force demands it. When you have a work force the size of the National Security Agency, if you didn't conduct yourself in accordance with the law you would be bound to be in conflict with someone's personal interest in the case of that agency and you would have whistle-blowing going on all over the place. Another good reason is that the agency is terribly important to our national security. Periodic findings of improper performance — by periodic I mean every five to ten years under one administration or another — would undercut its reputation and its credibility in the future. The agency is quite conscious of its credibility, and doesn't want that to happen.

Earlier, I mentioned the capabilities of the services in the context of SIGINT consolidation. Each service has cryptologic elements: In the Army, Navy, Air Force, and to a far lesser extent in the Marine Corps, there is a command for which the principal responsibility is cryptologic intelligence. In the Army's case, it's an even broader definition than that, but it includes cryptologic intelligence. In addition to having cryptologic elements, each service has organic assets, or specific cryptologic collection capabilities — actually, collection, processing, and analysis capabilities. While the technical tasking arrangements are good, the division of effort is imperfect. There is still room for improvement in administrating the collection and processing, in analyzing, and in disseminating the intelligence.

Oettinger: Are these service capabilities provided with service budgets, Department of Defense (DOD) budgets, or DCI budgets?

Faurer: There are four budget programs for which I have responsibility, and they fall under two major budgets. The consolidated cryptologic program (CCP) is our largest budget program. It deals with the full national SIGINT program as administrated by NSA. A much smaller program called the tactical cryptologic program (TCP) deals with cryptologic research and development to support eventual service procurement of cryptologic equipment for the tactical commander, principally in support of hostilities. It comes under a small budget called the tactical budget. The so-called national program — I dislike using that

word because I think it has the wrong connotation for what we do — may have application to a tactical commander, but it's designed to serve a national mission. The CCP, NSA's large program, is part of the National Foreign Intelligence Program. This is overseen by the Director of Central Intelligence, and contains the additional intelligence programs under which the DIA and certain reconnaissance programs operate. This budget, although administered by the DCI, is contained within the defense budget.

The tactical budget also falls under the defense budget, but is administered by the Secretary of Defense. For NSA it includes two others, a Communication Security Program and a Computer Security Program. So there is that split in budgeting responsibilities. The services obtain research and development (R&D) and cryptologic support out from either the National Foreign Intelligence Program of the DCI — my CCP — or from any of the other three programs under the defense budget. All of those budgets, incidentally, we build at the agency, we defend before the appropriate Congressional committees, and then administer, to the extent they are approved by the Congress.

Student: Is there an overlap between the collection of intelligence for tactical purposes and for national purposes?

Faurer: Yes, but that's the reason I am the program manager for both the large consolidated program — the so-called national approach to cryptologic intelligence — and the tactical-related TCP, to ensure that there is no inappropriate redundancy. I make sure that if the R&D we pay for in the CCP has tactical value, it is provided to the TCP.

Student: I'm not sure I understand what you mean by tactical versus national purposes....

Faurer: All right, let me take the easy half of that question first. Everything in direct contact with a battle, we think of as tactical. Tactical commanders operate forces to win battles.

Student: Regardless of where hostilities occur.

Faurer: Yes, regardless of where they take place — air, sea, or land. In a tactical environment forces move around, the enemy is engaged, and one attempts to win battles. The tactical commander has some intelligence assistance, some SIGINT assets that collect, process, and analyze right there on the scene.

The national intelligence apparatus is designed to gather intelligence for all of the government. It may have an application to the Commerce Department, the State Department, or the Defense Department. That is what I refer to as national, and that is the bulk of our program. As we gather intelligence under that national hat, it may have some application to the conduct of battle.

Over the last five to ten years there has been a dramatic increase in the applicability of national-derived intelligence to tactical commanders. That's because there's been an enormous time compression between the instant of collection and product usability. It used to be weeks, weeks gradually became days, and now it is seconds, minutes, and hours between the instant of obtaining intelligence and a usable product. Time compression alone has made national intelligence usable in a fast-moving, tactical situation.

I'm concentrating on SIGINT because that's my job. I acknowledge that there are other intelligence disciplines which also are considerably valuable in moving data to the tactical commander, which come into the C^3I equation, and which must be handled when solving problems associated with moving data. There is imagery (IMINT), there is human-derived intelligence (HUMINT), and each has advantages as well as limitations. HUMINT has a problem in timeliness. It's often difficult to move that human-acquired intelligence quickly back through the structure and out to a tactical commander. Imagery does not have a timeliness problem, but it has a volume problem. What is moved makes a great deal of difference in one's communications load. What is important is that the data be combined, and that we recognize the absolute necessity of interaction among all intelligence derived from the various disciplines. That is the crux of the C^3I problem.

How does all the derived intelligence flow together so that all is complementary, and then how is that combined answer moved to the appropriate decision maker? That process is being improved through applied automation and enhanced communication. The integration of automation and communication into tactical intelligence systems will ensure timely and meaningful exchange of the data. And I heartily endorse that occurrence. The issue becomes *where*, because it becomes a problem if extremely large amounts of data are generated that can saturate the decision maker. We're talking about all the SIGINT

in a battlefield situation and the imagery that might pertain to it or the human source of intelligence coming from the reconnaissance element.

Colonel Beckwith,* in writing about his experience in *Delta Force* (his book recounting the Iranian hostage crisis), makes much of the saturation problem. I don't think his is a perfect example, because it mostly discusses the saturation occurring prior to going in on the operation, but Beckwith addresses the problem of assembling all the pertinent intelligence, then having to sift through it to create a necessary picture.

The Long Commission Report** is an example from a slightly different direction. When they looked at the disaster of blown-up Marine barracks in Beirut, they strongly recommended that there be a fusion center to tailor and focus all source intelligence in support of military command. They argued that, stretched across the intelligence community, there had been quite a bit of potentially pertinent information prior to that terrorist attack, but it hadn't come together because there hadn't been a forced fusion of all pertinent intelligence.

What is this fusion we're talking about? There are a lot of definitions of fusion. Simply stated, it's the integration of multiple sources of intelligence. The real issue is not wasting time arguing about what fusion is, because it can mean different things to different people. The real issue is where the fusion should take place, and that, in my opinion, is the far more difficult question.

There are a number of automated fusion systems being developed or designed. Industry has a dozen or more potential systems that will digest intelligence information and present easy-to-use displays for commanders' decisions. Many voices in the services are asking industry to provide them with specific attacks on fusion. The various attempts at automated fusion systems are designed to provide battle information, or to censor data from multiple sources and combine that data. They're trying to provide near real-time enemy ground situation, display it, and make target nominations that a commander may choose to pursue.

---

*Col. Charlie A. Beckwith, USA (Ret.) and Donald Knox. *Delta Force.* New York: Harcourt, Brace, Jovanovich, 1983.

**U.S. Department of Defense, Commission on Beirut International Airport Terrorist Act, October 23, 1983, Admiral Robert L. Long, USN (Ret.), Chairman, *Report of December 20, 1983.*

20

They're trying to aid in assessing the enemy's situation and capabilities, and to assist a commander in using his organic sensors and jammers so he can manage them against that changing enemy target. And, these systems attempt to give him the insight to coordinate with higher echelons those sensors he needs assistance from, away from the battle.

Let me talk for a moment about SIGINT support to the military commander. A conflict exists between the desire of that commander to control his own assets, and maximum SIGINT support. Every commander will tell you he feels far more confident going into battle with control over both what will fight and what will support him. On the other hand, he currently does not have, and is unlikely to acquire (because of cost limitations) the intelligence wherewithal to fight that battle alone. The assets just can't be made available.

Student: Excuse me. Are there any of these fusion systems in the field now?

Faurer: Yes, we have a system in Europe called LOCE (Limited Operational Capability, Europe). It is a prototype system, an evolution of a system called BETA (Battlefield Exploitation and Target Acquisition System) that first saw the light of day in the late '70s. There are two systems somewhere between prototype and initial operating capability status called ASAS (All Source Analysis System) and ENSCE (Enemy Situation Correlation Element), which are Army and Air Force systems, respectively. So, yes, there are systems in existence. In addition, there are a number of usable systems that various contractors suggest be purchased.

Student: Is there interoperability among the systems — the services' systems? Is that necessary?

Faurer: Interoperability isn't as necessary among fusion devices. What is necessary is the assurance that intelligence can be entered into the fusion system easily and promptly. I'll touch on that in a moment, but all the intelligence one would like to handle within that fusion process doesn't lend itself equally to digital handling and digital display. Technical parametric data is very easily handled; its quantitative and can go into that display without much trouble, if one is dealing with radars and so forth. But if human-analyzed information is to be handled, it's much more difficult to enter and judge properly.

It's also difficult to enter data that raises the security level. There can be all kinds of problems with accessibility, working with the allies, and so on. If those fusion devices are to function in areas where not everyone is cleared for compartmented intelligence, then there is a problem inserting compartmented intelligence into the fusion system. Leaving it out does the fusion process great harm, but putting it in causes that SIGINT fragility problem.

Student: In the European theater, how important is NATO to interoperability and compatibility?

Faurer: It's terribly important. We haven't solved the C^3I-related problems that I'm talking about with respect to our own forces. When you compound the problems by trying to solve them so that we remain interoperable with allies, you have a solution that lies well ahead of us.

Student: Are these fusion devices basically a computer with an associated network?

Faurer: Yes.

Student: I'm not quite sure I understand the location of the fusion. It seems to me that before the fusion devices came about, who should get what information was clearly established. How does the technology change that organization?

Faurer: If there were no fusion devices, the basic problem of where the fusion should take place would still exist. Don't mix the issue of hardware with the philosophic issue of where the digestion, correlation, and coordination should take place. It is the latter problem that is the crux of the issue.

Student: So, it's not really a new problem.

Faurer: It is not a new problem, but it is accentuated by automation in the fusion process because it places a very disciplined demand on communications to move volumes of data. Before, all of the right intelligence may or may not have reached the right decision node, even though the problem of where the decision nodes were and to what intelligence they were entitled had been considered. Once carefully structured automation devices are available, there's a clearly defined tug on the intelligence system demanding that there be a communications flow to move data to certain nodal points. There is a clear trade-off between letting all the intelligence be assembled at one place, well out of theater where processing assets are optimally employed, and letting intelligence be processed out in front. If all intelligence is to flow

from wherever it's collected, and it all returns from the theater, is processed and analyzed, and is sent back out in tailored bullets to the levels of command that have bespoken a certain need, there can be a dynamic dialogue. One can tailor answers to needs. That is one measure of how to do it, and it will have a certain communications demand.

The communications demand of moving everything collected back to a central processing and analysis capability, and then sending data back in tailored form to the multiple users, must be measured. Conversely, doing everything forward could be optimized. The various collection capabilities could channel their immediate take into the theater to be processed, analyzed, and turned around there for the decision maker. If that's the method, there's obviously going to be a big tail of support people, computers, and capability forward, but communications will only need to cover a relatively short distance.

As I say, which is the best answer is not intuitive. I lean toward the centralization, intuitively, but I am not a proponent of either if one excludes the other. There should be more attention to accepting the sacrifice of the commander who wishes to control everything. But if one follows that route, one had better carefully measure the communications requirements to make sure that they are affordable.

Oettinger: Centralized or decentralized intelligence processing — this fusion — seems principally a technical trade-off problem, and correct me if you disagree with the following way of putting it: The question of "where fusion" is, in some respects, also a question of "whether." Ultimately fusion has to occur, if only in the commander's head. It seems to be a perennial question of whether fusion or where fusion, and the degree. There's the Pearl Harbor and Long Commission accusations for when not enough fusion occurs, stating that the intelligence was all out there, but it never got put together. If too much fusion occurs, then there are user complaints about others putting together or suppressing information without the authority to do so. This is not a technical matter; this is a philosophical matter. It's not just trade-offs between how much communications versus how much computing. In a deeper sense, this is a matter of how much delegation versus how much overload; how much trust versus how much understanding. I wonder if that's an accurate perception. Why is this such a perennial problem?

Faurer: I don't think it is an accurate perception. I do think your description illuminates a legitimate concern we ought to have. We should not try to present to the commander such digested intelligence that it may bias him in unwise directions. But I don't think that's necessary at all.

Perhaps I ought to back up. I think there are two major achievements to be obtained in the fusion process. The first is achieving the appropriate interaction among disciplines, to ensure that intelligence that starts to become evident in one discipline is used to task and target other disciplines. Then, you are truly functioning across your whole intelligence collection capability in a complementary way. That's the first benefit accrued from some level of fusion. You can compare a piece of intelligence with capabilities; at this early stage of fusion, you know what you have and what you don't have.

The second achievement or level, though, and one about which you're expressing the most concern, is that fusion should stop well short of producing finished intelligence. That's why I think the Long Commission report muddies the water, although it is, in part, valid because it addresses specifically the fusion center and the shortcoming of the local command in the Beirut situation. What was really needed there was better finished intelligence, and I don't think many of us believe that the Marine commander on the scene would have profited from having all the bits and pieces available to him when he determined that he was at risk. It might have sensitized him into doing some things differently, but the place where there should have been recognition of a need to do some specific things was at some center other than the one sitting in Beirut, in my opinion. The Long Commission may be right in suggesting such a center is essential, and there have been a lot of steps taken since then, in a terrorist context, trying to optimize the assembly of the bits and pieces to give as clear a picture as possible. We're a long way from getting pictures that are clear in the terrorist business. Where there are enough pieces of the puzzle to see what is there clearly, intelligence can be fused perhaps better than in Beirut.

I wouldn't encourage you to shy away from fusion out of a fear that putting that process someplace other than with the commander going to inhibit that commander from making his own tactical decisions. That's not my intention. In fact, part of the

22

benefit derived from the fusion devices being developed is not just to look at red data or intelligence data, but to be able to superimpose red data on blue displays so that the human mind is helped by having more than can be conjured up in one mind, such as the image of what is actually going on in the battlefield area. Where are the blue and red assets? How are they moving with respect to each other? What are their quantities in respect to each other?

Oettinger: May I reiterate what I believe you said to clarify my understanding? If we're talking about the identification of an object out there that is an airplane, then are you saying that there's nothing to be lost, but there is an enormous amount to be gained by fusion that would ensure the understanding that it is an airplane, regardless of whether the intelligence came from a sensor owned by this outfit or that outfit? When you say "finished intelligence," can one ascertain specifically whether that object, that airplane, is on a training mission, or is on an attack, or what is to be done to respond, and so on? That is in a somewhat different realm. Or is that still where you think second level fusion helpful? Where is the boundary between what you described as "finished intelligence" and the earlier forms?

Faurer: My use of the term "finished intelligence," of course, was designed to try to calm your concerns about an excessive delay at fusion centers — be they automated in their assistance, or the fusion accomplished by people. An example in the case of hostilities is this: You have the same worry that a front-line commander has, not just about the forces in front of him, but about the type of reinforcement actions that may be happening in the second echelon. He has the capability to call upon a system to do something for him concerning those second echelons that will pertain directly to the battle in front of him, if he has some knowledge of it.

Now, there are certain things that simply must take place as forces move up. You need not wait until there is a bridge down and troops are pouring across it to suspect strongly that there is a river crossing intended, and the distances are such that those forces will pertain to the battle in 18 hours. As those kinds of early indicators come in, one would like to see them seized upon: a potential river crossing identified, the correct tasking information sent out, and an air strike laid on that could strike four hours later at the height of their movement. With this example,

I'm suggesting that fusion is essential if you're to bring together the bits and pieces that will permit action to result. A commander need not worry that the collating of bits and pieces is occurring somewhere behind him. They need to be provided to him directly so he can decide whether or not he cares about that river crossing. He has got other problems: He may want to call for air support, which may not be the first thing to do, or he may want to send an enveloping tank column out. I don't want to intrude on his decision. I want to provide him with the intelligence as rapidly as I can; I do not want him to sit there with an intelligence staff and sort through a saturation of intelligence that will force him to arrive at his own conclusions. I believe one can tailor the intelligence provided to meet the demands a commander has expressed.

Student: General, as an operational aviator, I have a little bit of a problem with what is being proposed — not with the philosophic base of fusion, but with, first, the fact that it's so technologically deterministic, and second, that it seems to have a land war bias. Can you address both of those points, sir?

Faurer: I'm not sure I understand what you mean when you say "technologically deterministic."

Student: It's hardware, and any piece of hardware can be somehow glitched in a real crush....

Faurer: Yes, I'm sorry if I have caused you to think I am hardware-oriented to a fault. As I mentioned in an answer a moment ago, we should separate the issue of whether fusion results from automated systems or whether it occurs without automated systems — whether it is a group of people sitting in a room with a lot of communication lines in and out, providing them with data that can be correlated and then synthesized into tailored form for a commander. If you are more comfortable thinking that way because you don't trust hardware, that's okay with me.

The volume of data we are dealing with now and will surely deal with over the next decade suggests we can't do it without automation. We won't be able to handle the amount of pertinent information for displaying what the commander needs to know. So, I do not believe you should think I have disregarded human essentiality, because I have not. In fact, it's one of the reasons I come down slightly on the side of the fence that argues for fusion taking place predominantly back from the forward area, outside the

battlefield, because I want to make optimum use of the talented people who are available. If I must have a large intelligence staff with all command levels doing their own intelligence digestion, I am not likely to digest as well as if I can husband my more limited resources in more centralized places, and have the processing and analysis done at those places.

Concerning the aspect of ground and air: You may think it strange that an Air Force officer would have such a predominant flavor for explaining what he's talking about in terms of ground battle. It's easier, usually, but this audience may be different. Take an average audience of 15 people. They will grasp far more easily what is said about the ground environment on which we all walk, than they would a description of how air assets are juggled to achieve interdiction, or supremacy on the battlefield. The major difference that occurs between ground and air, frankly, is time. Intelligence must be far faster providing information to that air commander than to the ground command. Beyond that, there's not a tremendous difference.

Student: Who is the great beneficiary of the LOCE system, the commander at the battalion or S-2 level, the Army or G-2 level, or the U.S. Commander or J-2 level?

Faurer: It's interesting you would ask the question, because the answer you usually get depends on where the person being asked works, or for what the person is principally responsible. It applies to several levels, and my personal advocacy with respect to automation assisting the fusion process is that there is no single answer, a LOCE, or an ASAS, or an ENSCE. One should not try to develop a single fusion device and methodology to accommodate all levels. I believe they should be assembled in a more modular fashion that will emphasize separation and aggregation. That setup will permit certain amounts of fusion or aggregation at one location, and a different amount at another.

So, where does LOCE sit today? LOCE sits at the Air Force headquarters (USAFE) level in Europe. It is there to be used by a NATO command, but it sits physically at Ramstein Air Force Base in West Germany to be employed by either Allied Air Forces Central Europe (AAFCE) in the NATO context, or USAFE in the Air Force context. That's not necessarily the right place to put it, but it will do its job there if we can input all the intelligence properly. We can't

at the moment. We have great trouble putting our signals intelligence into it so that it will be properly in balance with the other intelligence going in.

Student: Is the Army deputy chief of staff for intelligence jealous of your capability?

Faurer: Of LOCE? The Army was not initially as supportive of LOCE being in theater as was the Air Force. I don't think that view still prevails; my sense of it is that both Army-Europe and Air Force-Europe are equally interested in the potential of the program. Both are pursuing the follow-on systems, ASAS and ENSCE, to come do the job for Army and Air Force, respectively. Besides, to ask if they are envious would suggest it's working so well that they wish they had it. And I don't suppose anybody in theater thinks it's working that well.

We've covered a great deal of what I planned to mention today. Allow me to talk for a couple more minutes, and then I'll get back into your questions. I hope, if nothing else, we've established that the problem of bringing together intelligence is complex, with the help of automation or otherwise. As I suggested in an answer to a previous question, the problem is exacerbated when the need to provide intelligence support is brought into the equation. Intelligence support creates interoperability between our command structure and that of the allies.

What are some of the problems with the system? Well, I alluded to the fact that when computers work outside special channels, the information that can be input is influenced. One way or another, you have to face up to that problem. If that computer remains outside, there must be a method to feed the computer the sanitized information. And, with sanitization, which may be essential, there is at least some delay imparted into the introduction of that intelligence to the computer system.

I said that narrative descriptions reduced to quantified data often lose their essence. Intelligence that has been produced to describe something is difficult to quantify and put in so that it will balance properly against the more mechanistic and technical data going in. At least at this time, machines don't make associations well. That's something that still lies in the future when we become more proficient at artificial intelligence.

Moreover, weighting is absolutely essential to analysis. All pieces of intelligence simply do not

have the same value. We'd like fusion assistance — that use of automation — to make it more likely to find the right answer. So, we must be capable of facing that weighting problem. It leaves a problem of how to introduce information into that device in such a manner that weighting is not ignored, and that everything doesn't come out weighted the same.

It's difficult to verify information once it's entered into the computer. Some control over the ability to manipulate is lost, and it's difficult to maintain a data base and perform quality control at the same time. This is particularly true in fast-breaking situations — crises or war fighting. One can move data quickly, but maintaining a consistent data base and running quality control may be more than one can handle.

What are some of the ways to improve this? Well, the process can be reversed, and can be selective in collection and processing so that the input is constrained by some responsible analytical decision process. It doesn't have to be performed by humans, but it has to be an achievable, responsible analytic process. One can tailor the reporting at the collection end for substance, format, and timeliness. That also can be done, to some extent, with computers as opposed to people. With properly programmed software, different characteristics of an event may be converted to a set of common features and values if one can properly forecast what sort of intelligence is to be assimilated. However that is done — and I hope it's some solace to you — analysts are still essential to the process. There's no question about that. Analysts have to assess the significance of an event; they've got to update the battlefield picture because they're dealing with both red and blue data, and irrelevant data must be discarded. And the information has to be weighted. All of those things can be done to some extent by machines, but not sufficiently, and not with an adequate degree of perfection.

I told you that there were two concepts of how to manage that information and make it useful. You may have direct delivery from the source in SIGINT channels, where the tactical commander correlates the data and produces his own intelligence. That puts a pretty good-size tail there, allowing him to do that. Or, you can have an all-source intelligence center that tailors the intelligence to different user categories.

There are advantages to both the direct delivery and the intermediate nodes. I emphasize intermediate nodes because one must not think only of choosing between the proliferation of decision nodal points attendant to each tactical commander on the one hand, and one central processing pie-in-the-sky on the other. There certainly may be some redundancy, but the nodal points should remain back out of theater or be responsible for segments of the theater. That's still something different from having them with each tactical decision level. Those intermediate nodes, or that sort of centralized processing, surely provide more economy of resources. One is better able to monitor the overall success of the system, and one is better able to know the disposition of enemy and friendly forces. I don't think either complete centralization or complete redundancy is the sole answer. I believe there is a middle ground.

We at NSA can and do contribute guidance on the use of SIGINT data in the fusion process. We've become more aggressive in the last six to eight months in dealing with fusion design and the fusion automation designers, so that we can discuss selective targeting with them. We can suggest ways to achieve a programmed reduction of the amount of information collected, rather than collecting everything. We can talk to them about tailored reporting. We can discuss that in terms of substance, format, timeliness, or the nature of operations. All of this matters when determining what automation device will help the fusion process. If we are to evolve an optimal fusion design that will assist the intelligence process and provide timely intelligence to the customer, it is going to take performance by more than industry, by more than the operational user, and by more than just the NSA or the intelligence community.

Unfortunately all three of us, private industry, the tactical commander, and the NSA, bring a particular bias to the debate. I first contend we all must sit down and work very hard together, but I concede that each of us has a significant bias. Private industry is obviously after a profit. It wants to sell something marketable and attractive, that sounds like it will do absolutely everything. The operational user or the tactical commander has an insatiable appetite for information. The tactical commander would provide a list of what is needed to conduct battle. This list would become so long, it would not be possible to provide a commander with that amount of intelli-

gence. It's very difficult to get back to talking about essentials.

We at NSA have a security bias. We're more interested in protecting — or we appear in many instances to be more interested in protecting — the security of our intelligence than we are in providing intelligence. That probably is an excessive allegation, but it certainly appears that way. We simply recognize those biases and recognize the need for all of us to talk, particularly to industry. We're trying to be as aggressive in marketing our concepts as we can justify. I have the total NSA responsibility to interact with the military customer, to be the bridge between those military customers and the rest of the agency, and to be the catalyst within the agency for provoking problem-solving ideas.

For example, we have started inviting commands into our agency. We have what we call command days, when we invite a command like USAFE or Southern Command from Panama to spend a day with us. During these meetings, they tell us what they need and we tell them what the capabilities of the SIGINT system are. On the second day, the commander usually leaves while most of the other folks stay, and we break off into one-on-one sessions. These provide a very helpful dialogue; we understand better what they need, and they suddenly understand what this SIGINT system can do for them.

McLaughlin: I'd like some differentiation in some of your examples of military customers. It seems to me there's a question of whether or not you're talking to a CINC as opposed to a TAC* commander, a component commander. Who is the real customer?

Faurer: Are you suggesting that we might be talking to too high a level as we try to find out what the military customer would want?

McLaughlin: No, I'm not suggesting that at all. I'm wondering how much you are under pressure to satisfy a customer who represents component commanders from the services versus the CINCs.

Faurer: There are some different perspectives at the two headquarters. We hope to talk to both. We'll consult, for example, the commands we have in USAFE or TAC, both headed by Air Force commanders, or in SOUTHCOM, headed by a unified

---

*Tactical Air Command, the Air Force component command in U.S. Readiness Command (REDCOM).

commander. We're quite prepared to talk to both, because both are important.

Unified command in Europe has to be the voice speaking for the unified hat. If you talk to Air Force-Europe or Army-Europe, and certainly if you talk to Navy-Europe, you will receive a very parochial view of the battle, and understandably so. Their programming is designed to be parochial. Each of our services' programs for a structure seem as essential to the conduct of hostilities as to the preservation of deterrence. But the unified commander is the one who steps back from it all and looks at the integrated battle that's going to have to be conducted.

For example, in Europe or in Korea at the present time, and just starting in the Southern Command and the Central Command, there are intelligence architectures being developed in which there are attempts by the intelligence and operations people to look at the intentions for war-fighting in the next decade, and to decide — given that the war will be fought by our concepts and our intentions — what kind of intelligence support will be required. So, as each of the services then goes back and builds individual budgets, and we, at an agency like NSA, build our individual budgets, we all are likely to do it in a coherent way to produce the right total intelligence capability in that theater.

The possibility that we, perhaps, are not talking to the right level is not an easy problem to overcome. I had occasion to visit Europe last fall, and while there, talked to some corps spokesmen (I won't identify which corps). I was very annoyed that in this European ongoing intelligence architecture context the corps felt that they had no time to participate. They were simply so overwhelmed with staying afloat on a day-to-day basis that they did not believe they could devote any energy to the articulation of intelligence needs and the desirable intelligence posture for the next decade. That's too bad, but it's a fact of life. The alternative is to go back up the chain and talk to the commands, and hope that they have a reasonable insight into what their divisions, corps, and wings need.

McLaughlin: You do wonder what the corps would do in war, if the headquarters is that hard-pressed in peacetime.

Faurer: Well, they would tell you — so that I don't sound like I'm entirely opposed to those corps for

26

that attitude — that they are spending an awful lot of peacetime trying to be ready for war. They do a lot of exercises, a lot of training. They also write a lot of papers that find their way to Washington from there. We don't overly man the staff levels of our fighting outfits. The TO really mans the staff of fighting outfits to fight, not to cope with the problems of peacetime — paperwork, planning, budgeting, or concept development. It takes less people to fight than it does to exist in peacetime, unfortunately. You and I may not like that, but I do believe that's true.

I guess the last thing I would simply comment on concerning what we've been pushing at the agency, in this context, is exercise. I do believe the only way to find out, in truth, how things will operate, and, therefore, what should be changed and improved in the C^3I arena, is to exercise realistically, and that doesn't come free.

In fact, to address this issue of available time, if you take time out to play war, i.e., exercise, you've got to stop doing your peacetime thing. You can only afford to stop doing that so often. We are trying very hard at the agency to be more supportive of realistic exercises and to encourage the forces to be more realistic in their military exercises. We encourage getting away from merely scripting alone in the case of intelligence, and getting down to actually making intelligence systems work, making intelligence staffs work, making communications and support of intelligence flow work, and finding out where the realistic shortcomings are, so we can do something about them.

McLaughlin: General, on that point, how realistically can you exercise without giving away something?

Faurer: You can't exercise without giving away something. We work very hard at studying Soviet exercises. They work very hard at studying our exercises. We constantly ask ourselves, "Are they going to fight the way they exercise, or are we being deceived?"

They undoubtedly will ask themselves the same question. But the bottom line is, you can't go out and perform on Sunday if you haven't practiced all week. You can toss in a few little wrinkles, but you really must have practiced what you're going to fight, and so you give away a little, but that's necessary. You can go a long way towards protecting the insight

into specific capabilities that I spoke of earlier if you are careful with your operations security, and careful with your communications security during the conduct of exercises. We are not adequately careful at the present time, and our analysis of our security violations while we conduct operations is somewhat sobering. But that's a correctable deficiency. The lesson to be learned from that is not to stop exercising, but to start exercising better so you don't give too much away in exercises. Then you won't give it away in wartime.

Student: When you address the fragility of SIGINT about providing the intelligence from these fusion centers during hostilities, the assumption is that all the data collected in peacetime is also available to us during hostilities. That seems to be incorrect. Rather, wouldn't the data be dramatically reduced? How is this accounted for during exercises? How do you model a situation wherein there is much reduced capability?

Faurer: Unfortunately, our exercises are not that sophisticated. To my knowledge, we have not spent much time trying to forecast capability attrition in a sophisticated way, or imposed upon ourselves the most likely attrition that will occur in wartime. We happened upon a certain amount of realism by our very inability to operate simultaneously in peacetime and wartime.

So when we exercise, we quickly clog our communications and make it difficult to move data. We find ourselves artificially constrained from having all the information we're trying to pass, so that in a somewhat obscure fashion, we can say we've imposed some realism on ourselves, but not intentionally. We have not thought this constrained situation through and imposed it in a methodic way. That is something yet to be done, and the need for far more realistic exercising than we now do requires a carefully orchestrated capability attrition. You're right in suggesting that there will be a dramatic difference between that intelligence available to us in real war from that available to us in peacetime, but it isn't all in one direction, I would hasten to add.

There will be some things the enemy will deny us in wartime. By the same token, he also will have to act in a much more precipitous and high volume fashion in wartime. There'll be a lot more equipment on the air, a lot more activity occurring in the electronic intelligence area — radars emanating and so

on — and there will be a lot more communications taking place. He, and unfortunately for us, we, won't be able to rely entirely on secure communications. There'll be a tendency to force information flow. There's a trade-off both ways. I think we would be well advised to make some assumptions and to introduce some carefully imposed constraints into our exercises.

Student: General, you've addressed most of your comments to the tactical theater and battlefield using intelligence and communications. I wonder if you could address the problems with fusion on the national level in a crisis. How is fusion accomplished and how well? Could it be improved?

Faurer: I guess I would start by giving ourselves a report card that says we rate somewhere between fair and good, at the national level, in providing essential and appropriate intelligence to these decision points. However, I don't think we're optimally structured to create the decision points. I would fault us a bit there though I think there have been definite improvements in the last ten years.

There's been some profitable thought on how to handle the national decision process. I don't think, at the present time, that we have adequate national intelligence survivability to guarantee flow to our decision makers. I think, perhaps, our greatest failing lies in our cultural reluctance to accept the imminent possibility of war starting. That probably is not only big war with the Soviet Union, but war at almost any level in a crisis. I think we will be reluctant to accept the indications that say someone is going to start shooting shortly. Therefore, we will lose the advantage of action that might precede that first shot, for fear that by taking action we will worsen the situation and encourage hostilities. Having been involved in the national scene since the early '70s, I certainly could point to lots of things that I think have improved, but we still have a long way to go.

Student: General, I'd like to follow up on the question of bias mentioned earlier but in broader context. Over the years, different components of the Washington intelligence community won the reputation of having certain biases. One reads about the different perceptions of service attitudes toward specific issues like Backfire, for example. In your tenure, sir, what have been the most troublesome biases associated with NSA prevalent in Washington? And, what are you going to do about them?

Faurer: That's sort of an invitation for considerable dirty linen washing, and I don't know whether I want to take up the offer completely. Let me approach it in a slightly different way from the way you asked.

A very often voiced criticism of the CIA, for example, and by spillover sometimes the DCI, who is both head of the CIA and head of the intelligence community, is that the CIA is overly policy-attentive. Allegedly, the CIA tends to produce national intelligence designed to complement the policy makers' desires. Over the years when I have operated in the national scene that has occasionally been a justified criticism, not as often as it is made, but occasionally. It is not a valid criticism over the past four years, despite its having been made often about Mr. Casey and the current CIA.

You see, even the most well-intentioned of the intelligence community, as they prepare estimates or advise the policy maker, must have an eye on the policy maker's interests. That is, not what conclusions he ought to reach, but in what he ought to be interested, or in what he is interested. As an estimate is put together, it is essential that certain aspects not be overlooked in regard to a problem that the policy maker clearly needs to confront. In doing that, one occasionally provides the policy maker with exactly the kind of information he wants, because he's made up his mind in advance about what he wants the answer to be. And just as often that does not happen. When it does, the screams go up about playing into the hands of policy makers. I simply have not seen it happen. I believe the community has operated during the last four years with considerable integrity.

Pertinent to this question is the role that the DCI plays. You will find advocates of a DCI who is isolated from the administration; you will find those who would say, "Let's have a professional agency, an employee as the head of the agency, and let's not bring in a political appointee each time the administration changes."

That would probably guarantee you maximum objectivity on the part of the DCI, but it would give you a DCI who might not have the ear of the President and the administration, and, therefore, would be disadvantaged in helping the policy makers because he wouldn't be a part of that policy in the first place. I think the best of all worlds is to have a political appointee, if that's how you would refer to

a Mr. Casey, who does have the ear of the President and who is thoroughly aware of the administration's deliberations and policy development, yet who also has the intellectual integrity to stay aloof from pandering and oversees a community that he demands put together intelligence pertinent to the issues at hand without trying to color it. I don't know how many people like that there are around.

You must have divined by now I happen to be a supporter of Mr. Casey. I think we have one such man at the moment. And he is probably the best kind of DCI to have.

The DIA frequently gets put into a conflicting position with the CIA. Remember, the DIA has a bias of its own, in that it is designed exclusively to provide support for military structures, whereas the CIA is trying to cater to all government emphasis on national policy, foreign policy, the State Department, and other government agencies as well. That sometimes causes the DIA to view intelligence through a different hue of glass than does the CIA. It is helpful that they serve as a hair shirt requiring strong argument on the CIA's part to prevail on a given issue, but I don't find the conflict as harmful as the media sometimes makes it.

Take a case in point right now. The media has made a major issue out of the CIA and DIA differing on the rate of Soviet commitment to defense. If one reads nothing but the headlines, and even some of the careless text that follows those headlines, one would think there was a markedly different perspective held by the two agencies. Well, there is not.

Both agencies agree that the more important measurement is not the rate of growth of the Soviet commitment to defense purchases, but rather the amount of military force acquisition and the increases occurring in it. In other words, it is the product of that expenditure that is important, not its rate. So, the CIA and DIA tried to come out with a statement for the press to clarify their agreed posture. I noticed that received somewhat less play and still biased headlines, but in truth, as I listened to both talk, there is nowhere near the gap between them that the media suggests.

There is some difference, however. Helpful relations occur because of those two agencies. The DIA has somewhat of a bias coming out of the military, and I would stop my criticism of the DIA at that

point. The NSA does have a bias, as I conceded earlier, towards the security area.

At my request a retired professional colleague and good friend of mine went around the community trying to find out how we could improve the image we have acquired over the last three and a half years. Largely, our bad image derives from the suspicion of all sorts of intelligence agencies like the CIA, DIA, and other smaller entities that we are so obsessed with security that we sometimes hold onto intelligence. They charge we don't make it available until we can get a headline by doing it quietly ourselves. I wouldn't say that we deserve to go off scot-free on that allegation, but it is a misperception. We don't hold onto intelligence; we simply do not always share it as freely or as clearly as others would like, but we do share the essence of all that is important. There's a difference.

We don't hold onto any intelligence that needs to be passed on to some consumer who has stated a requirement. We'll find a way to get it to that consumer. We'll sanitize it, we'll hand deliver it, we'll do something; we don't hold onto anything. But we will not turn over to all analysts all intelligence that we come by, because of the simple matter of SIGINT fragility that I spoke of earlier.

Student: Sir, would you mind addressing the security issue with respect to leaks? About three weeks ago in the *New Republic* an investigator wrote that he thought there was too much classified in the government, which is a criticism we hear a lot in the military and from the inside, also. And this morning, in Anderson's column in the *Washington Post*, it was reported that an investigator checked up on some top secret papers that the President wouldn't quote last week in his press conference. If it's that easy to get hold of even sensitive, compartmented information, I know some of us must not be doing our jobs right. Would you care to address that particular issue?

Faurer: I could wax eloquent or attempt to be eloquent for an hour or two on the subject of leaks, which I consider abhorrent. I listened to a very edifying TV clip a year and a half or so ago, using a corporate broadcasting service that staged a forum. Typical of these forums, a moderator was named, people were invited in from both sides of the issue, and a discussion ensued — a very effective means to discuss an issue. I watched one that discussed intelli-

gence and leaks, or classified information and leaks. It had prominent newsmen like Dan Rather and others arguing the media side, and it had a few government officials present and past — James Schlesinger and others — on the government side.

Over the course of that discussion, there were some terribly pointed questions asked, and a couple remained rather clearly in my mind. One was that the media has almost unanimously suggested that it is government's burden to protect classified information, and it is media's obligation to the public to obtain it by any means possible. That includes specific statements by some of those media people sitting there on camera, saying that if they were in the Secretary of Defense's office for a legitimate purpose and saw an opportunity to take a top secret document off his desk, they would take it and use it. I have trouble understanding that. Dan Rather himself said, that if provided with clearly classified information — stamped classified — and if it pertained to a story he felt needed telling, he would use it. He would feel uninhibited about using it. I don't understand that.

A while ago I mentioned meetings that I've been having with managing editors from publications such as *U.S. News & World Report, Newsweek, The New York Times* — that level of publication. During one of these sessions I was having lunch with one gentleman, and we were trying to understand each other's position on the Cuban missile crisis. I was trying to understand what he thought his obligation to the public was. I asked him what his response would be to the following situation: Our government was preparing for an invasion of an island that would use U.S. forces, and had done all of the things required by law with respect to Congress — they had forewarned the Congressional leaders, and they had managed to keep this event secret — and it was going to take place in a few days. If he or one of his reporters became aware of that, would he think it appropriate to break that story? He told me, yes.

I said, "If you do that, one of two things will happen: Either the administration will go ahead with the invasion and American lives will be lost, by virtue of the loss of surprise. Or, the course of history might be changed." I don't mean to sound over-dramatic, but one does not ordinarily go around planning invasions unless there's some terribly important foreign policy reason, at least in the administration's mind.

"No," he said, "Even though as you hypothesize, the government had done everything it was supposed to do — the executive element of the government cross-checked with the legislative element and they had done what the law required — that isn't enough. Governments can't be trusted. Only the people must have the ultimate say in what the United States does on a major scale like going to war."

I don't understand how we can survive in that kind of world. It worries me a great deal. I — and simple little sensitization attempts like mine, of pointing out the importance in World War II of the kind of capability we protected — don't seem to carry the day since we regularly try to give away such capabilities with the leaks to the press. I feel rather strongly that if we are going to err on the subject of protection of classified information, we are better served nationally in erring on the side of over-classification. Now, I understand that as governments come and go, both parties' government leaders tend to misuse classification on occasion. When they want to declassify something, they do, and when they want to hide behind classification, they do. I guess that's an evil we've got to live with. I don't think the fact that this happens occasionally justifies the promiscuity with which the media is willing to use classified information. I do think it obligates and justifies the media constantly attacking government for misusing its own classification. But I think that's where the permission stops.

Student: Sometimes the leaks that you're referring to come from the highest levels of government itself. The case I've been thinking of is the Korean Airliner 007 (KAL-007) shoot-down.

Faurer: That wasn't a leak.

Student: But it was a disclosure of certain intelligence methods....

Faurer: Yes, but that was not a leak. And, I don't suggest that the average reader of the paper is always going to know which is a leak and which is not a leak. I was just saying I don't condone a government using classified information to serve its policy purposes. So, I'm probably on your side of the argument on that.

There is a third category. There is the leaking that the media generates because they've extracted some information from somebody. There is the leaking that occurs because people in government deliberately do it, either for their policy reasons or for self-

aggrandizement. Then there is the other category of disclosure, and the KAL-007 is such an instance. Here a conscious government decision was made openly and acknowledged that it was necessary to share classified information with the public to make the public understand the enormity of an event. And in the case of that airliner shoot-down, neither the American public nor the international public would have believed the President of the United States if, with a mere assertion, he had said that an airliner that disappeared several hours ago, and of which no one knew the whereabouts, was shot down by the Soviet Union in the dark. I don't think anybody would have believed him.

Student: Are you saying there's a certain weighing process that has to go on?

Faurer: I think there comes a time when events of certain enormity demand sufficient disclosure to make them understood by the public. I think that was such a case. The appropriate people within our government were contacted, the disclosures were discussed, their completeness approved, and the story was nearly as exact as it unfolded. Nothing of any significance was kept from the public in that instance.

Student: You spoke a little about the complexities of integrating intelligence capabilities in NATO. Can you be a little bit more specific about it? How can LOCE or USAFE capabilities be made available to the European command, and how are capabilities integrated, at what command level?

Faurer: I can. I'm not sure that a detailed tutorial on the manner in which intelligence support will flow will be helpful to you, because it varies as I told you — perhaps unfortunately — but it varies, at the moment, just on the U.S. side alone. Each service has its own idea of where decisions should take place, where the intelligence decision nodes should be, and each theater looks at it differently.

When the allies are introduced you add still another perturbation in Europe. When we dealt with BETA, the forerunner of LOCE, one of our greatest difficulties in setting up a test environment was the nonparallelism between the Air Force and Army fighting structures. It would be nice if one could draw organizational diagrams that would fairly parallel decisions for size units and nature of the battle and so on, but it doesn't work that way. The Air Force and Army

have quite different structures, so I don't know whether I'd serve your purpose by trying to cover all the services in my answer to your question.

I will tell you what they are working toward. Both services in Europe concede that the European battle will be fought in the NATO context. It is unlikely that U.S. forces alone will find themselves fighting a war in Europe. So, it's essential that there be created an adequate, integrated structure for the conduct of war in allied command Europe, headed by SACEUR General Bernard Rogers, and populated by U.S. and other general and flag officers throughout a NATO structure. But that structure is a very soft, peacetime structure that seldom, if ever, exercises itself in any large scale in wartime. It exercises itself in what you might call CPX's (Command Post Exercises), nonreal movement of forces. It's conducting one right now called WINTEX — but that's not quite the same as moving people and fleshing out command structures. All the U.S. services agree that any war needs to be fought in the NATO context. The trouble is, that introduces all kinds of problems on a daily basis.

There isn't enough of a sufficiently fleshed out NATO structure, populated by NATO people, to function in peacetime as it would in wartime. It's a skeleton force that, in wartime, will have to be fleshed out by people coming in from somewhere, with nations pouring in more intelligence information, suddenly making communications lines available: A number of quick jerry-rigged things will have to be done in order for NATO suddenly to become a war-fighting machine.

Student: So, is part of what you're saying that you would prefer a centralized fusion center if you had to make the choice of both? You said that there were advantages there. But now you're suggesting that the way NATO would function in war is actually more decentralized....

Faurer: Where I'm going with the line I'm on at the moment is that I favor centralization even for our U.S. force structure, though I could sanction and support a certain amount of decentralized, forward analysis, and immediate provision of intelligence. The preponderance of fusion for the U.S. structure should be done in a centralized way. I'm suggesting that if the dimension of trying to fight war in a NATO context is added to that problem, it becomes all the more important to try to do it from a centralized place. It's going to be much easier and more

practical for this NATO war-fighting machine to surface requirements back, and receive intelligence satisfaction out of intermediate nodes or more centralized nodes, than it will be to flow all intelligence — some of it at highly compartmented levels — throughout a NATO structure that is multinational. We are uneasy doing it in our U.S. structure alone. It boggles my mind that we think we could flow that intelligence into foreign command structures as well. I think we can flow it through an integrated command structure if it can be tailored, and if it can respond to stated requirements. But I don't think you can just dump a full flow of intelligence forward and have sufficient interoperability to cope with it.

Student: Are you saying it would be decentralized and informal and somewhat nonhierarchical because of the nature of the NATO command structure?

Faurer: It would be compounded by security problems, or inadequate cross-communications; to me a number of things would make it impossible to create a fairly even flow of knowledge.

Student: So, how much does our ability to communicate during conflict in the European theater concern you?

Faurer: We are unable to communicate adequately at the present time, but that's not a secret to anybody. We know that, although you might get arguments if you tried to describe the amount of shortcoming. What is the optimum solution? Where should we spend our money next? What should we do most immediately to improve our communications?

You'd get different answers from different people, but you wouldn't get an answer from anybody that suggests our communications are adequate for the conduct of war in any theater. They aren't adequate in Europe, they aren't adequate in Korea, and probably border on potential inadequacy even to support the national decision process attendant to war fighting. We know that, and we know that there are a lot of initiatives under way addressing it. Again, I'm not disclosing anything with which anyone would disagree. I do not know whether we can make an adequate financial commitment to correct that, as the study effort starts to describe more specifically what could be done.

Student: What are your first priorities for improvement?

Faurer: Our first priorities? We can be more selfish than others and, at the moment, we are and have been for a long time. Our approach is to ensure adequate communications for moving our data in peacetime, to try gradually to make that more robust so it can survive some encroachment in wartime, but our real hope lies in reducing the essential. And the lesson we preach on this subject isn't how much more communication to buy, although we're happy to do that even though the figure is large, but rather our lesson is the essentiality of reducing the identification of the requirements.