INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Intelligence: Cult, Craft, or Business?
Charles E. Allen

Guest Presentations, Spring 2000
Charles E. Allen, Albert J. Edmonds, John J. Garstka, Timothy G. Hoechst, Hans Mark, Dale W. Meyerrose, Mark C. Montgomery, Scott A. Snook

July 2001

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
ISBN 1-879716-74-7 **I-01-1**

July 2001

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Anonymous Startup
AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz•Allen & Hamilton, Inc.
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
Critical Path
CyraCom International
DACOM (Korea)
ETRI (Korea)
Fujitsu Research Institute (Japan)
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
High Acre Systems, Inc.
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
NMC/Northwestern University
PDS Consulting
PetaData Holdings, Inc.
Research Institute of Telecommunications and Economics (Japan)
Samara Associates
Sonexis
Strategy Assistance Services
United States Government:
  Department of Commerce
    National Telecommunications and Information Administration
  Department of Defense
    National Defense University
  Department of Health and Human Services
    National Library of Medicine
  Department of the Treasury
    Office of the Comptroller of the Currency
  Federal Communications Commission
  National Security Agency
  United States Postal Service
Upoc
Verizon

Intelligence: Cult, Craft, or Business?

Charles E. Allen
April 6, 2000

Charles E. Allen was appointed assistant director of central intelligence [ADCI] for collection, Central Intelligence Agency [CIA], in June 1998. In this capacity, he is responsible for managing collection and requirements for the intelligence community. He also chairs the National Intelligence Collection Board, which ensures that collection is integrated and coordinated across the intelligence community. He has served with the CIA since 1958, holding a variety of positions of increasing responsibility, both analytic and managerial. From 1974–77, he served overseas in an intelligence liaison capacity, and from 1977–80 held management positions in the Directorate of Intelligence. From 1980 to November 1982, he managed a major classified program until he was detailed to the Office of the Secretary of Defense, where he held a senior position in strategic mobilization planning. In 1985, he returned to the CIA as national intelligence officer [NIO] for counterterrorism, representing the director of central intelligence [DCI] on the Interagency Intelligence Committee on Terrorism, which he chaired, the Interdepartmental Group on Terrorism, and the National Security Council Terrorist Incident Working Group. In February 1986, he was also appointed chief of intelligence in the CIA's new Counterterrorist Center. As the NIO for warning from 1988–94, he was the principal advisor to the DCI on national-level warning intelligence and chaired the intelligence community's Warning Committee. He has received the National Intelligence Medal for Achievement and the President's Award for Distinguished Federal Civilian Service, and in 1991 he was awarded the CIA Commendation Medal for providing warning intelligence in Desert Shield/Desert Storm.

Oettinger: What I want to underscore about Mr. Allen is that when you looked at his biography, you may have noted that he was at one time the national intelligence officer for warning. If you're interested in that subject and have something to say about it, I want to point you to one of his predecessors, David McManis, who appeared at this seminar a couple of times. So, if you want to compare the recent past with the longer ago past in that particular position, remember that there are a couple of occurrences of David McManis in these seminar proceedings.[1] With that, Charlie, it's all yours.

[1] David Y. McManis, "Warning as a Peacekeeping Mechanism," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1984* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-85-2, February 1985); "National Security and the 'Democratization' of Information," in *Guest Presentations,*

Allen: Thank you very much, Tony. It's a pleasure to be up here and to be out of Washington, even for a few hours, and the bureaucratic imperatives that go on there on an hour-to-hour, day-to-day basis. This is a place where we speak in an unclassified forum, and the work that I do is, of course, inherently classified. That is, we protect things that generally work best when known to ourselves and not to our adversaries, so you'll bear with me in the way I talk about certain issues. I'll certainly talk about the issues, processes, and principles involved, but it's hard for me to talk specifically about certain items.

I want to talk a little bit about things that have some policy relevance, but I want to speak mainly about the art and craft of intelligence and only touch lightly on the business aspects. I guess with Tony here it's sort of imposing. We could have talked about the science of intelligence, but, by and large, as far as I'm concerned the science of intelligence is yet to be invented. I don't see it. It's not really there.

But I think, more than ever, from our perspective, from the administration's perspective, and from the Congress's perspective, our national security depends on good intelligence. The next generation of smart weapons, the greater likelihood that we'll be faced with information warfare in the future, the multipolar environment of the world, and the transnational complexities all demand more and better intelligence. We've just been discussing it at lunch. We've not quite transformed ourselves to meet those new challenges and those new complexities.

It's clear that more scientific discipline is needed to underpin our work, but, as I said earlier, that has yet to be invented. In looking at the materials that Tony sent me about the Program on Information Resources Policy, I was struck by the graphics that plotted things on axes without scales. The axes ran from products to services, from form to substance, from prescriptive to descriptive. I think in some sense that's the way intelligence is, because as we practice it, intelligence generally resists strong scale types, too. Our data are more singular, and we are generally unable—and, I think, in many cases unwilling—to apply more formal methods. One of the things that we really need to do is to help the intelligence community develop methods that attach value to products.

We're able to measure what intelligence products cost in terms of persons and person hours, in terms of dollars, and, sometimes, even in lives. We also can measure the number of bits we collect or the bandwidth we consume in transmitting our products. We are unable to quantify the value of our products. There's sort of an interesting question as to why this is, because isn't intelligence just information in its purest sense? Why can't we measure its value as it affects the policy decisionmaking process?

Of course, the rub is that sometimes very good intelligence is unable to affect policy decisions. Foreign policy decisions are constrained by variables that have little to do with intelligence and a lot to do with agreements, international law, treaties, domestic politics, costs, military capabilities, and the like. In many cases, good intelligence can lead to little action other than handwringing. We may simply have no options, or we don't have the political will to act on

Spring 1989 (I-90-3, August 1990); and "Technology, Intelligence and Command," in *Guest Presentations, Spring 1991* (I-93-1, February 1993); all available [On-line]. URL: http://www.pirp.harvard.edu/pubs.html that intelligence. It’s as though intelligence at times is akin to medical screening for an incurable disease.

We’re not very good at evaluating the quality of intelligence analysis independent of the outcome. We’re outcome oriented, rather than process oriented. For example, getting back to the whole question of warning, consider an event of some consequence (**Table 1**). Either the event is favorable and was predicted correctly by intelligence, or unfavorable and was not. It leads to the four alternatives you have here. If there’s a favorable outcome, there’s kudos for intelligence if it’s predicted correctly. If it’s not predicted, the policymaker, likely as not, takes credit for it. Sometimes, even when we’re very successful in something, the policymaker will take credit for it without any regard for intelligence. If it’s an unfavorable outcome—if the event occurs and we don’t predict it—boy, there is truly a tendency to punish the innocent, as I see it. The press and, particularly, policymakers tend to look for so-called “intelligence failure.” Frankly, what is billed as an intelligence failure might just as well be a policy failure.

Table 1

The Cross-Product of Favorable and Unfavorable Outcomes, with Accurate or Failed Predictions

	Predicted Correctly	**Not Predicted**
Favorable Outcome	Kudos to intelligence; cursory, self-congratulatory post-mortem that mistakes the quality of the outcome for the quality of intelligence.	Seen as a credit to the policymakers; generally there is no intelligence post-mortem…the sentiment is to let well enough alone.
Unfavorable Outcome	Despite a willingness to punish the innocent, we feel good. The patient died, but the operation was a success.	Intense post-mortem of the "intelligence failure," where collection and analysis attempt to allocate blame to each other.

Conversely, when the policy succeeds and a desirable outcome occurs, we feel satisfied with the conduct of intelligence and generally look no further. The cumulative effect of this process is that it undermines the very essence of intelligence analysis.

These are the questions that I think are absolutely to be rigorously asked:

- What set of hypotheses was being considered? Was the set comprehensive, or was there bias in the selection of hypotheses? What *a priori* probability was attached to each hypothesis? Again, was there bias?
- Was there a good understanding as to which observables would differentiate between the hypotheses? Was intelligence collection requested on the basis of these differentially diagnostic observables?
- Were all of the then-available data considered? How were the data weighted? What degree of credibility was accorded the sources?
- Was the possibility of deception considered and accounted for?

- Was the analytic process logically correct? Was the confidence in rendered judgments correctly estimated? If so, and if the confidence was low, was additional collection requested?
- Were the judgments presented in a timely and adequate manner?
- And, of course (my area of concern), was intelligence collection responsive and timely?

Only by answering these questions can we really continue to improve the quality of intelligence analysis. The implication is that intelligence should be dispassionate in relation to the resultant policy outcomes. Intelligence may sometimes succeed in the face of policy failure, and policy can sometimes triumph in spite of intelligence.

As I said earlier, sometimes intelligence is like medical screening for an incurable disease: the diagnosis may be accurate, even though the prognosis is grim. There may be simply nothing that a policymaker can do to change an outcome, despite perfect knowledge. Harry Rowen,[2] a rather well-known figure in Washington, would argue that in August 1990, because of the mindset at the policy level, even with the best of warning nothing could have changed the actual diplomatic or political measures taken by the administration promptly enough to avoid the invasion of Iraq.

The policymaker is constrained by the laws of physics, sometimes by the principles of economics, and frequently by the will of the body politic. One of the challenges we have is that we need to think about how to formalize the assessment of the value added by intelligence, regardless of policy consequences.

Oettinger: If I might just break in for a moment, that last set of comments I think is very profound and applicable to the business world as well. The problem of staff advice to a decisionmaker is a recurrent one, and simply punishing or rewarding people according to the outcome leads to some strange results in business as well as in the government. I think it’s worth your taking these remarks to heart, not only in this context but also applied much more broadly.

Allen: As some of you know, I served as the NIO for warning from 1988 to 1994. My job was to alert policymakers to pending critical events: to sound the klaxon. In the world of warning, we distinguish between strategic and tactical warning. The main difference, of course, is the time horizon. The cynic would say that strategic warning is far enough away that we don’t have to worry about it, and that tactical warning means that we don’t have time to do anything about it because it’s too late. Our goal, of course, as with intelligence, is to support U.S. policymakers by providing as early a warning as possible. But this is not without peril for the warning officer, because if he raises a false alarm and the crisis doesn’t eventuate, then we truly have a problem. On the other hand, he perhaps faces being fired if he doesn’t warn about it.

We certainly had an episode in May 1998. There was an explosion in the Thar Desert in India, as you may recall, where nuclear devices were set off. There was a great deal of review in Washington on that particular issue. The most memorable example for me occurred in the summer of 1990, because there was enough warning. I had been warning very strongly of threats

[2] Harry Rowen, former chairman of the National Intelligence Council and former president of the RAND Corp.

to the Arabian Peninsula from Saddam Hussein. I was personally convinced by the third week in July that there was going to be an absolute takedown of the government of Kuwait. All the signs were there. I have a whole lecture I give on the invasion of Kuwait.

I did sound the warning bell, and, surprisingly, there were very few listeners on the other side. I was accused of being an alarmist. I issued a warning of war in July, and I issued a warning of attack in late July. I felt a little vindicated a couple of weeks later, and no one said that I was wrong, as they had earlier in the summer. But I wasn't hailed very much either, because the outcome was unwelcome. Unwelcome outcomes are frequently something that a warning officer faces.

The necessary relationship of false alarms to correct predictions or misses is poorly perceived by the policymakers and not well understood by all people who call themselves warning practitioners. Let's review another chart (**Table 2**). If a warning is sounded about a critical event or not, and the critical event either occurs or it doesn't, we have four cases, as shown here. It's a hit if it's a warning success, even if it is a policy nightmare. If the warning is not given, then it's a failure. It could have high national consequences. Certainly, it's very costly to the warning officer. You might also have a false alarm, or a false positive. That's viewed, of course, as a failure. It may give respite for the policy-weary, but it could be rather costly. Sometimes it's very hard to distinguish between warning success and simple oversight.

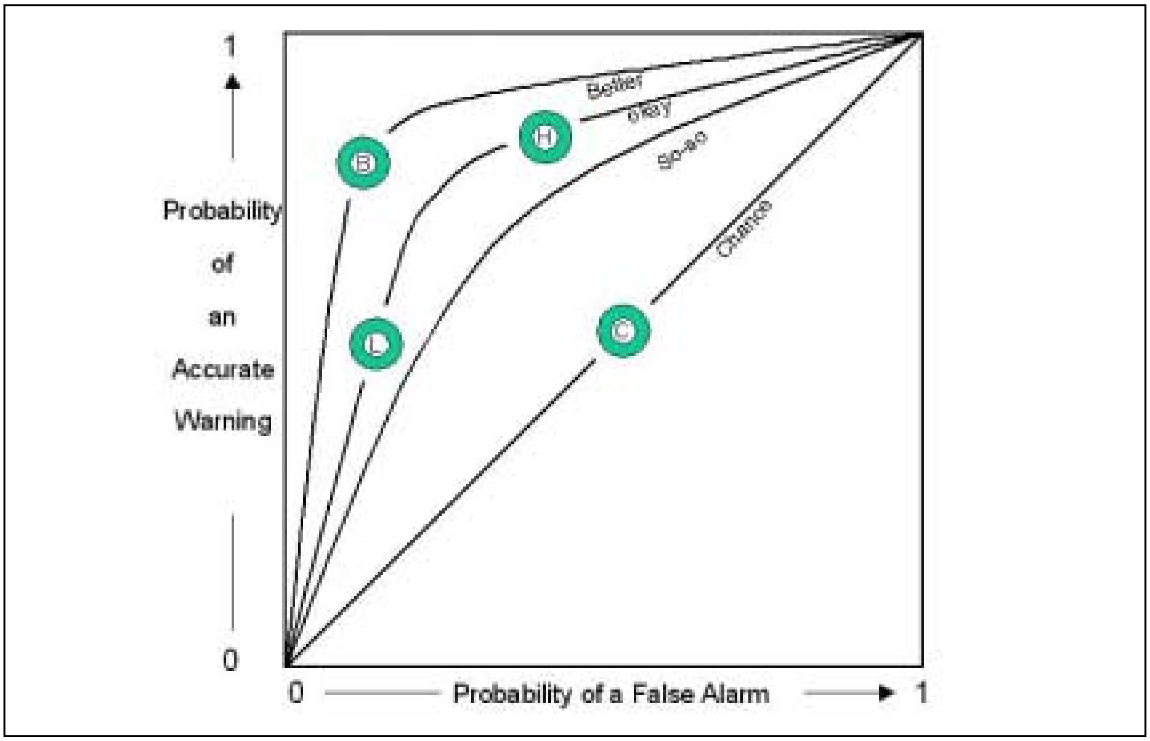
My concept of warning is that you warn early, you base that warning on reliable data, and you warn in a successive fashion. Warning is not an event in time. Warning is a continuum. That truly is not thought about very often.

Table 2

Relationship of False Alarms to Correct Predictions

	Critical Event Occurs	**Critical Event Does Not Occur**
Warning is sounded	A "hit"—a warning success, even if a policy nightmare. The value may depend on policy options.	A "false alarm" or "false positive"—a warning failure, perhaps a respite for the policy-weary, but could be costly.
Warning is not sounded	A "miss"—a warning failure which may have high national cost, and is surely costly to the warning officer.	"Fat, dumb and happy"—distinguishing between a warning success and simple oversight is hard.

The next graphic is rather interesting (**Figure 1**). What policymakers and warning analysts must continually relearn is that there is a tradeoff relationship between the probability of false alarm and the probability of accurate warning. It is really important to understand this. If you look at case C, it's sort of 50–50, where you could do just as well by flipping a coin. I hope our warnings are never that poor. But let's look at case H and case L. Those two are terribly important. They lie on the same curve, which means that they indicate equally strong warning performance. The difference is that in the case of L the threshold of the warning officer has been effectively raised, so that he or she does not issue that warning as often and so the likelihood that this person will be inaccurate in warning is lower. In the case of H, there is a greater likelihood of error, of raising a false alarm, but there is also a greater likelihood that you're going to make a more accurate prediction.



Trading relationship between false alarms and accurate warnings. Point C indicates performance no better than flipping a coin. Points L and H represent equivalent performance, their difference due to changes in "criterion" that can be influenced by the "costs" and "values" associated with predicting or missing the critical event, and by the a priori likelihood of the event. Point B represents better performance and could be influenced to move along the curve by the same factors.

Figure 1

On this line, I tended to stand at H. Someone said we need at times to dampen the ardor of warning. My view is that we need to lean forward to be able to avoid consequences to the United States. By doing that, I tended to lean somewhat forward to get the policy-level thinking about an issue in different terms early. That's generally the way we in the intelligence community operate today.

If the consequence of a false alarm is "missiles away" or the belittlement of an analyst who cried wolf, then the threshold is inevitably going to go up. If the consequence of failure to warn is "Off with his head!" the threshold tends to go down. Note that these payoffs may be unspoken and perhaps unintended, but no less insidiously effective.

The effect of the likelihood of a critical event in question can be similarly subtle. When we are at peace, the unexpected is doubly so. If, on the other hand, we're in continuous engagement, we're primed to expect the unexpected. The hair trigger is set.

In the case of the Thar Desert explosion, we were not ready for that as a government, at the policy level, or in the intelligence community. Now, of course, with the potential for increased nuclear developments in both Pakistan and India, let me say that it would not be unexpected. The threshold is higher, so if the warning comes, policymakers will be far more ready for it, and far more receptive to it.

The policymakers were not at all receptive to the warning in the summer of 1990. For eight years there had been subtle support of the government of Iraq or, more precisely, not so subtle support against the theocratic regime in Iran. So there was no receptivity on the part of policymakers to any warnings. Many simply thought that Saddam Hussein was going to bluff, that all he needed was liquidity. He was getting attention, and he needed some funding support from the Saudis, Kuwaitis, and others. It's this same kind of effect that causes warnings to be taken seriously or to be ignored, as they would be when issued by a warning analyst who is known for crying wolf, for exaggerating every threat, or for seeing a bogeyman behind every bush.

Returning to the figure for a moment, consider how we might move warning performance from a lower curve to a higher, better curve. As we have seen, we cannot do it by abusing the warning officers. What we must do is recruit better human sources, take higher resolution photography, listen in on the right communications, and improve analytic methodologies, including warning methodology. These are things that we're trying to do in the intelligence community, as some of you know. This is easier said than done, but it's important to focus on the information that underpins the warning, not on the personality of the warning officer.

I'd like to talk a little bit about intelligence as a business, which Tim Hoechst and others will have an interest in. It's become fashionable to suggest that the government should function in a more businesslike manner. This is plausible on the surface, but it attaches too much significance to the business metaphor. Government, in the final analysis, differs significantly from business. A government function cannot be entirely responsive to market forces. Government functions are assigned by statute. We cannot simply choose to abandon an unprofitable line and redirect resources to another, more lucrative area. Indeed, functions are frequently assigned to government precisely because they're *not* economic but, instead, serve some higher public welfare purpose.

So I think it's important to ask: "What is the core business of intelligence?" One view is that the intelligence mission, simply stated, is to fully inform those who make and execute national security policy. However lofty it may be, this notion is challenged by those who have heard the siren song of the business metaphor. They argue that the competitive advantage of, and, thus, the niche market for, intelligence is the ability to steal secrets. Consequently, the core business is to harvest those secrets and to market them to consumers: to policymakers and the military. Organizationally, this is an argument about the primacy of collection vis-à-vis analysis. The spillover to collection, where I work all day, is the argument as to the value of open sources and the resources that should be devoted to exploiting them.

I'd like to talk a little bit about open sources, because I have very strong views on this that are not necessarily supported by even some of my colleagues around the community. Former DCIs, from Allen Dulles to John Deutch, have acknowledged the value of open sources in answering the information needs of policymakers. Yet they tend to diverge as to the proper role of open source intelligence in the business of intelligence. Is it a core business area, or is it in some ways external to the intelligence process?

I'd like to contrast the views of former DCI Robert Gates and former DCI Deutch. Bob Gates places open source in the forefront of the intelligence process, and I quote from a paper he wrote: "The community needs to create an 'open source gateway' through which all new policymaker requirements must enter, so a determination can be made how much of the information requested is already available openly."[3]

Dr. Deutch puts open source somewhat differently. He says, "The community must strive to assure that the President and other leaders of the nation have the best information available before making decisions.… Providing these judgments requires both the collection and the analysis of secret information, but also the integration with increasingly public information."[4]

Now, is open source a source of first resort or an afterthought? Taken too literally—and I don't say that this is their final position—the advice of either DCI would lead us astray. Bob Gates's position could be interpreted as seeking no further if open sources were to supply a plausible answer to a policymaker's question. But if you stopped in mid-analysis, as it were, how would you know that the conclusions at which you arrived were not contradicted by secret information? A similar flaw would be Dr. Deutch's relegation of the use of open source to a backdrop for purloined secrets.

The dichotomy posed by the advice of these respected DCIs mirrors the feckless efforts to calculate the value added by each intelligence discipline or, as we call them in Washington, INT. It is no more meaningful to ask, "Given the HUMINT [human intelligence] we collect, of what added value is open source?" than it is to ask, "Given the open sources, of what added value is HUMINT or any other intelligence discipline?"

Another matter for you to think about is that we do really require a new calculus for value added concurrently, not successively. Nor can we forget that multiple sources of information are required to pierce the veil of deception. From my point of view, open source has been, is, and will always be a core capability of U.S. intelligence. It should be the source of first resort, because it does present the baseline for global, political, social, and economic trends. It serves as a tripwire for impending crises in countries normally of less interest and focus for the U.S. policymakers, and it provides the infrastructure details in support of military operations. It's the reason we see the CINCs [commanders in chief] are quite interested these days in building open source databases. The collection of open source information at relatively low cost allows the intelligence community to reserve riskier, more expensive collectors for truly secret information.

Open source represents less than 1 percent of the U.S. intelligence budget. It is very small indeed. Open source in my view undergirds other intelligence collection disciplines: HUMINT, SIGINT [signals intelligence], and IMINT [imagery intelligence]. It serves as a launch pad for operations, a tip-off for collection, and the context for interpretation.

[3] Robert M. Gates, "A Leaner, Keener CIA," *The Washington Post*, Jan. 30, 1995, p. A15.

[4] John Deutch, testimony before the Senate Select Committee on Intelligence, June 21, 1995.

The DCI’s National Intelligence Collection Board provides a forum for the exchange of information across collection disciplines. I chair that board. It’s composed of the intelligence community’s most senior managers in collection. We meet two to three times a week, face to face or by teleconference. The Board truly does influence collection, particularly near-term collection. Every time I prepare an intelligence collection posture statement or an assessment for the DCI, I ensure that the functional manager for open source is sitting at my right hand. He is extraordinarily key. I guess I get rather emotional when it comes to the open source world. This is one job that I believe has not been done right by the intelligence managers over the years, and I think it needs far more infusion of funds.

Student: Is the central manager for open sources this year the COSPO director?

Allen: It used to be the COSPO director. COSPO—the Community Open Source Program—no longer exists. Dr. Joe Markowitz ran that for several years. He had, I thought, a brilliant program. Because of cost-cutting, it was essentially abandoned in 1998. The functional manager for open source is the director of the Foreign Broadcast Information Service [FBIS]. He sits with me on my collection board, because all the functional managers sit on my board. In that way, we can ensure that their tip-offs are integrated into what we do, but, in all candor, there’s a lot of additional work to do.

We’re taking another look at open source within the community, and a new open source steering committee is being formed, with a rotating leadership. The first head will be the director of FBIS. That committee is going to report to me, and things are probably going to change as long as I’m around. We’ll get a little more energy out of the open source world and, we hope, a little more funding from the program and budget people and from the Congress. If you go to Congress, which I do frequently, there is a lot of support for this.

I would like to talk a little bit about requirements—a subject that is debated endlessly in the intelligence community. We refer to requirements all the time. We tinker with the requirements process. If we aren’t doing another study in the intelligence community on requirements, then we really are not doing our job, because it seems that we have had endless studies within the various intelligence disciplines and within the various agencies.

Generally, I think these studies and their efforts have foundered on the presumption that we can establish a single prioritized list of requirements that can be used for everything from tasking collectors to balancing the budgets of agencies in the intelligence community. I think that assumption is fallacious. I’m sure that there are plenty of other people who would disagree with that statement within the community.

DCI Jim Woolsey (and he’s a very good friend of mine) acknowledged the fallacy when he shunned the use of the word “requirements.” He rejected it; he substituted the term “information needs.” I think some useful distinctions can be drawn between the information needs themselves and their respective priorities. We must also distinguish between short-term and long-term needs, and I think Jim Woolsey did that. He talked about “information gaps,” which in the near term means simply stimulating additional collection. He also used another term frequently, “enduring challenges,” which engender the need for additional intelligence collection capabilities. Those needs get us into acquisition, which is something our colleagues in the Pentagon know to some degree.

Oettinger: Could you amplify a little bit? Perhaps you're heading in that way. "Needs" or "requirements" imply articulation by someone, and that someone could be either the intelligence process and a kind of supply push, or it could be the customer and some kind of demand pull. I wonder if you could elaborate on that a little bit more.

Allen: I'm going to speak to that a little bit further on. But in my view—and I want to be responsive—we have to be customer oriented. My counterpart, John Gannon, who is the ADCI for analysis and production, works with the user community. I define the user community as the issue coordinators—those who either functionally or geographically have responsibilities for all sorts of intelligence production and the heads of what we might call the production centers: the production center at the Defense Intelligence Agency and the production center at CIA, which is the Directorate of Intelligence. He also has the responsibility to deal with the policymakers, with the people within State, the National Security Council [NSC], the policy people at Defense, and perhaps even Treasury.

I'll speak a little bit more about how I see that system working. It has not worked well in the past. Anyone with a lot of experience within the U.S. government knows that in the past we frequently simply built collection systems and then found users for the systems. We try to do that a little differently now. We try to set up core system acquisition. We have within the intelligence community the equivalent of the JROC, the Joint Requirements Oversight Council. It is called the Mission Requirements Board, established by the DCI, which looks at long-term acquisition capabilities, five to fifteen years out. Who sits on that Mission Requirements Board? I sit as a vice chair, along with John Gannon, who is also a vice chair. But it's people representing the interests of the users. The Department of State sits on it; the NSC does not sit on it, but CIA, reflecting the requirements of the NSC staff, sits on it. The people who work on transnational issues in the production centers sit on it. So, we have a better process for doing business, in lieu of no process, which is what we had up until last year.

Student: When was that started?

Allen: The Mission Requirements Board was established in August 1999, and it meets monthly.

Student: Did you look to the JROC as an example?

Allen: It's not nearly as large as the JROC, with its massive staff.

Oettinger: JROC is described in a couple of past sessions.[5] So you ought to find a cross-reference there.

[5] See, for example, from *Seminar on Intelligence, Command, and Control, Guest Presentations* (Cambridge, Mass.: Harvard University Program on Information Resources Policy), Robert T. Herres, "The Role of the Joint Chiefs after the 1986 Defense Reorganization Act," in *Guest Presentations, Spring 1989* (I-90-3, August 1990); Joseph S. Toma, "C^3: A View from inside the Joint Staff," in *Guest Presentations, Spring 1991* (I-93-1, February 1993); William A. Owens, "The Three Revolutions in Military Affairs," in *Guest Presentations, Spring 1995* (I-96-2, January 1996); and

Student: I guess the issue would be that we hope the JROC is forcing us to buy inherently joint systems.

Allen: You put your finger on the real question. In most cases, there will be significant compatibility in future acquisitions, but I also have some comments here on the national tactical interface and differing perceptions. We can talk about that. I think there will be differences.

There is the Interagency Senior Steering Group, which was established and chaired by the deputy DCI for community management, by the J-8 [Force Structure], and by the assistant secretary for command, control, communications, and intelligence in the Office of the Secretary of Defense. If there are differences over whether we should buy capability X as opposed to Y, they will come together in the Interagency Senior Steering Group, which is trichaired, as I mentioned. Then, if there are still differences in what we should buy, the secretary of defense and the DCI have to reconcile/solve that when it comes to programming resources.

We do have a better process, because until recently, in the post-cold war period, where the military has become a great consumer of national assets (and I'll have some comments on that), there was a true dichotomy developing, where the national mission was not expressing the needs of the national consumers in an articulate way. Now we have a better system, and I think it will work. It's got to prove itself. That's going to take several years.

Student: I hate to bring this down to a more basic level, but we have a number of people in the class who are not U.S. government and some who are not even U.S. citizens. Could you give us some examples of well-expressed requirements, so they get a good lock on what we're talking about when we say "requirements oversight"?

Allen: The foreign intelligence requirements—and that's what we focus on—stem from specific questions posed in those areas by users, starting with the president and going through the NSC. They are expressed in presidential documentation as well as in requirements that come from the secretary of state, the secretary of defense, or the chairman of the Joint Chiefs of Staff as needs for specific prioritized information on issues or threats to U.S. national security. What the intelligence community has to do is take those very broad documents and turn them into specific requirements, both geographic and functional. For functional, we're talking about counter-terrorism or counternarcotics—some things that are very major players.

Within that, how should we prioritize collection systems? Which collection systems? I have a little bit to say about that, because sometimes we're competing among ourselves for some systems. You need an extremely high priority to use certain collection systems. Maybe they're national technical means[6] and you have equal priority, but the capacity of that system can only serve one or partially serve the other. I believe that sometimes the competition is about properly optimizing those collection systems.

Robert A. Rosenberg, "Defense Science Board Recommendations on Information Architecture for the Battlefield," in *Guest Presentations, Spring 1996* (I-97-1, January 1997); all available [On-line]. URL: http://www.pirp.harvard.edu/pubs.html

[6] "National technical means" refers to intelligence satellites.

Student: As an example, would a requirement be that the commander in chief of the Pacific forces wants to know if North Korea is going to develop nuclear weapons?

Allen: That would certainly be a big requirement, but that requirement would also be encapsulated in higher level requirements at the presidential level, which are approved by the National Security Council.

Student: So a requirement might be: We want to know if Indonesia is again becoming destabilized.

Allen: Political instability would be a requirement, absolutely.

Pure information needs, free of excess doctrinal baggage, are relatively easy to deal with. Shopping provides an analogy. Sometimes we know what we want; sometimes we don’t. A knowledgeable salesperson helps. The customers express their desires. The vendor offers up what’s in stock that fits. Sometimes things are placed on back order; that is, they require additional collection. Occasionally, there’s nothing in the current product line that fits the bill. Additional collection capabilities are required. There are a lot of things we can’t get. We’re always looking for new capabilities.

The free-market analogy is imperfect in this case, because the customer, if this is a free market, is usually the one who pays for it (**Figure 2**). In this case, it’s the collectors, the vendors. It’s the U.S. intelligence community that has the resources, which, of course, are constrained.

I think the model we want to use is a rationing model, because frequently requests for information contend with one another for the collector’s resources. In the case of scarcity, with no transactional price to the customer, we impose a prioritization scheme that involves assigning (at a very large bureaucratic cost) a priority to each information need expressed. Indeed, this is the prioritization that could be said to transform a need into a requirement. Ideally, the priority should be given so as to resolve contentions, and in accordance with the importance of the request rather than the putative importance of the requestor.

I think we overdo the requirements process, trying to impose it across the board. Getting back to what I said earlier, I think we ignore the granularity of the contention for collection resources. An alternative, of course, would be to turn the consumers into customers who vote directly with their own dollars. I can assure you here that the consumers are not going to be paying for U.S. intelligence. Mort Halperin once talked to me at some length about why we have so much trouble funding U.S. intelligence.[7] It’s because all the customers, the people who should be paying for all this, are paying virtually nothing. It is in the defense budget, but if you go to the rest of the entire U.S. government, it’s always looked on as a free good. For that reason, policymakers, at whatever level, are always anxious for more information, always anxious for

[7] Morton H. Halperin, currently director of the policy planning staff, U.S. Department of State, served as special assistant to the president and senior director for democracy on the NSC, 1994–96.

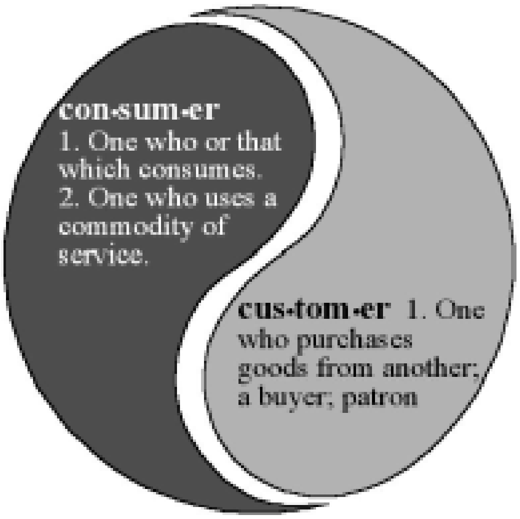

con•sum•er
1. One who or that which consumes.
2. One who uses a commodity of service.
cus•tom•er 1. One who purchases goods from another; a buyer; patron

Figure 2

more intelligence. It doesn’t cost them anything out of their budgets, so it’s always that free good. I think it’s an interesting way to look at the issue.

Intuitively, we realize that the actual contention for information depends upon specific collection mechanisms. The seriousness of the contention depends on the opportunity costs for that collection mechanism. Contention can occur because of orbital geometries; I was talking earlier about national technical means. We may have two very high priorities but the capacity to collect only for one of them, or only for similar language groups. We have a terrible time in the U.S. intelligence community finding enough linguists to process the information. There is a tremendous contention where we have high priorities for linguists to process, exploit, and report out information, but we have sometimes to make very hard decisions. Some things that should be accorded high priority fall on the cutting-room floor, simply because we don’t have the linguists to do it.

Then why are we surprised that global prioritization of information needs is of limited value? I think of more value is the prioritization of specific taskings for a specific collection mechanism and specific collectors. Until this point is better understood and more universally acknowledged, ambitious designs that are the be-all and end-all, 1-through-*n* requirements, are sort of feckless.

In my role as assistant DCI for collection, I work closely with my counterpart, John Gannon (**Figure 3**). Getting back to Tony’s questions, he helps to establish the needs and their priorities—in fact, to use Jim Woolsey’s phrase, the “intelligence needs.” My job, of course, is then to translate these into collection strategies that will really work. When prioritization is required, John provides a coordinated view of their relative importance. My responsibility, which takes up where his leaves off, is to ensure that the diverse collection apparatus of the community is harnessed effectively to meet those needs.

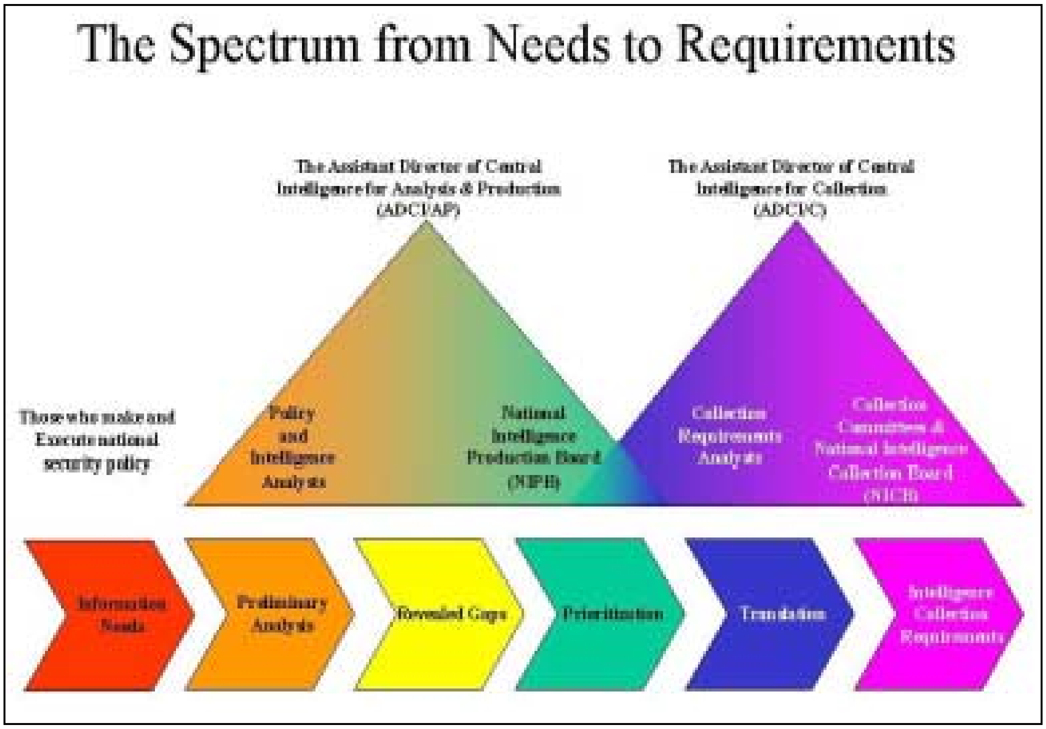

The Spectrum from Needs to Requirements
The Assistant Director of Central Intelligence for Analysis & Production (ADCI/AP)
The Assistant Director of Central Intelligence for Collection (ADCI/C)
Those who make and Execute national security policy
Policy and Intelligence Analysts
National Intelligence Production Board (NIPB)
Collection Requirements Analysts
Collection Committees & National Intelligence Collection Board (NICB)
Information Needs
Preliminary Analysis
Revealed Gaps
Prioritization
Translation
Intelligence Collection Requirements

Figure 3

Oettinger: Could I query you about what I see as another layer of complexity and contention there? Again, stop me if you're going to get into this later. I think I heard you say that your customers are, in a sense, Gannon's analysts. Did I hear that accurately?

Allen: Not just the all-source analysts, but particularly the issue coordinators, who have either regional or functional responsibility for the intelligence community—the NIOs. But the inputs have to come from the policy level. They come from the NSC, and they also come from the civil government, the non-national level.

Oettinger: But the latter, when they're knowledgeable, are sometimes in conflict among themselves as to whether they are buying the output of all of this at retail or whether they're going in and purchasing it wholesale or right down at the mine, instead of waiting for the manufactured goods. That sometimes, in my observation, generates a fair amount of contention and controversy. Am I looking at this through a window that you don't recognize, or a small window that's irrelevant, or is that a problem?

Allen: I think that really is a problem, because, yes, the customer may come in adjusted to the retail level or he may want it wholesale, and it differs from customer to customer. I'd say the military—the military commanders and the joint chiefs of staff—truly want it wholesale. They want it repetitively every day, whereas I would say that [National Security Advisor] Sandy Berger wants highly specific and sometimes very tactical information. He wants retail. He wants to be able to get a specific product. So that does add to the complexity. It adds to the exhaustion of the collectors and the collection capabilities. Trying to satisfy both is extraordinarily hard. I do have some comments on the national-tactical interface, which I think I should turn to now, given the earlier question.

Student: When you put up this picture, I actually expected to see it the other way first.

Allen: That I would drive the collection?

Student: Maybe I think that collection just happens on an ongoing basis, and then the analysis side decides what to do with that collection. But I know that a lot of it is tasked. So the question is, do you see your product going back to Gannon's organization? Or do you see your product going to someone else?

Allen: I see that my product goes to the all-source production centers, but it could be very quick tactical information that would go directly to the policy level. We have all read about this, since it's been reported extensively, where the national security advisor (not necessarily Sandy Berger), or the deputy national security advisor (not necessarily Jim Steinberg) becomes his own analyst. They want quick, raw intelligence because they have their own opinions. In fact, they know where they want to go. As you say, they want only a very specific retail product, to use the analogy that Tony used. So it's both. That adds to the complexity. It adds to the requirements process, the tasking process, the processing. Right now, the timeliness is required for both.

Oettinger: But could you develop that scene a little more? If a Berger or a somebody somewhere down the chain from the CINC picks up the phone and says, "I have yea or yea happening," that sets up a kind of instantaneous…

Student: Ad hoc requirements versus standing requirements…

Oettinger: Whichever way you want to phrase it, how do you handle that?

Allen: That's the jargon we use.

Student: It's a term of art, ad hoc versus standing.

Allen: The question is, how do we cope and do this well? I don't think we do it very well at all in many cases. Some of this gets back to the reality that ad hoc tasking tends to consume us, because our intelligence community and our administration have become very engaged globally. When we had a more static adversary, the Soviet Union, which was truly a great threat to our national security, wherever there were Soviets, wherever there were Soviet interests, wherever there were Soviet activities, we pursued them through every collection means possible. We were not whipsawed. We had Vietnam, of course, and things like that, but we were not whipsawed day to day with the diversity of tactical, ad hoc requirements we have today. We went through a significant reduction in personnel and budget in the U.S. intelligence community in the post-cold war. The giant superpower of the Soviet Union had ended. It was felt we could harvest a great deal of the so-called "peace dividend." What we now find, and Tony has depicted it well, is that we had some very false illusions about the nature of the world and the threats in that world. So we find ourselves not well equipped to deal with those, and particularly by the (should I say) insatiable desire of the military commanders for intelligence. No military commander ever has sufficient intelligence.

Student: And he is his own analyst by upbringing.

Oettinger: Before you go on to the national-tactical interface...

Allen: Let's pursue this, because this is bothering you.

Oettinger: Yes, let me again take a sort of business and technology analogy to see how it flies in this context. Henry Ford, among other things, became famous for saying, "You can have your car any color you want as long as it's black," and so he achieved certain economies of production, et cetera. That wouldn't fly in today's market, partly because the technology is there to let me pick up the phone, or go to Ford's Web site, or walk in the showroom, and say, "I want a car in *this* color and with *this* widget," et cetera, and they will make one for me. They can do that at a reasonable price, because the technology of production permits it. We're given the question as to which drove which—whether the possibility drove the market or vice versa—but there it is. So there is this problem of the ad hoc requirement versus the standing requirement, and the answer seems to be that you can have any color you want as long as it's black. Now, can technology, whether in the form of hardware or organizational ideas and so on, ease this question so you can say, "Okay, we can tailor it now. Maybe we couldn't tailor it fifty years ago, but today we can." To what degree can we do that?

Allen: I'd say Tim [Hoechst] could probably answer the question almost better than I can, because I think information technology is going to be the answer for a lot of our problems or, at least, will ease some of the pain that we have today. We tailor our product very quickly today. We publish our product very quickly, but our ability to collect intelligence, even human source intelligence, and particularly technical intelligence, is so overwhelming that we find that we can't process what we collect. We only process a small portion of it. We can't exploit it, we can't disseminate it rapidly, and we have a very sparse set of what we call linguists, traffic analysts, or reporters. There have to be some people in the loop, but, as you know, the community has been left somewhat behind the speed and capacity of collection. The new systems, as they come on, are going to have infinitely greater collection capacities. We're not there.

Oettinger: But that's like telling me that even though I can't sell cars, I'm going to continue to buy chassis and stack them up in my warehouse.

Allen: I want Tim to answer that.

Timothy Hoechst:[8] In my mind, it's more policy than technology per se that we're processing. It's one of the things that gives me heartburn.

Allen: It's policy to a large degree.

Hoechst: Yes, and business practice. Early on you made a comment that the government isn't a business. I totally agree with that. You can't just make a one-to-one analogy between the two of them; however, there are lots of things in which it could operate like a business, and this is one space in which I see that. So, at the risk of stretching your analogy beyond the breaking point, if

[8] Timothy G. Hoechst, who spoke immediately after Charles Allen, sat in on this presentation.

you are a retail store, you don't differentiate between your customers. By that I mean you never say no, and you don't charge them, right?

Allen: We seldom say no. I remember sitting with George Tenet and, I believe, one of our senior officials, now retired a second time, Jack Diamond. He said, "Why don't we say no, George?" Jack is very famous and has written in the press a lot, so I'm not telling you any secrets. George looked at him and said, "Well, *you* go down and tell that particular senior official you're not going to help him!"

Hoechst: That's right. Ford's strategy was never to say no, just to say yes his way. So if someone comes into your store and says, "I want what's on the rack," you say, "Great, it's free. Here you go." But if someone comes into your store and says, "I want a custom-made suit," you say, "Great, it's free. Here you go."

Allen: We do that every day!

Hoechst: And one costs a lot more to do. Granted, if the President comes in and says, "I need a custom-made suit right now," he gets it.

Allen: And he should.

Hoechst: But the question is, how many custom-made suits are you remaking for people who may not have been at the highest priority because of this always saying yes? Sometimes we don't differentiate between the cost of doing the different forms.

Oettinger: You're going to charge Mrs. Murphy's boy and girl out there in Kosovo?

Hoechst: I argue that you don't have to actually charge them. All you have to do is track and publish the costs.

Student: Admiral Jacoby, who is now director of military intelligence (the J-2), made his name at Pacific Command by saying no to the J-5. The other parts of the staff would come along and say, "We want you to give us an economic analysis of the Pacific Command." He said, "Read the *Economist*, read the *Wall Street Journal*, but I'm not going to do it."

Allen: My passion for open sources is really because for a few pennies we could make life a lot easier. The CINCs actually want open source for baseline data, to keep in databases and keep good and current. But I think technology can help, and we're turning this around slowly, as you know.

Our biggest acronym, which has been written up in the press, is TPED: tasking, processing, exploitation, and dissemination. The volume, and the tremendous capacities of technical collection today, are just phenomenal. We need to put more money into machine translation. I run a new center that is looking at what Jim Woolsey said are the enduring challenges. Ambassador Lynn Hansen runs it, and he's facing a very tough challenge.[9] He found fifty boxes of foreign language materials that no one's translated, which he thinks were very relevant. He says, "Why

[9] Lynn M. Hansen, U.S. ambassador to the Commission for Security and Cooperation in Europe, 1992–93.

haven’t we done this? This was really incredible material!” Well, we don’t have anyone to translate it. We need technology to help us in a lot of ways. To think we have fifty boxes of really sensitive information on a subject of real concern to the policy level, and we can’t translate it, because we don’t have anybody who can do it is sort of astonishing, but it’s a fact.

We have some military colleagues here, so let’s talk a little bit about the national-tactical interface. This is one that I just spoke on the other day.

This has been a real change. We’ve come a long way since 1990, when Colin Powell had to tell General Schwarzkopf that he really did need to have downlink capability for certain technical collection systems. Schwarzkopf didn’t think he needed it in those days. Today, the military depends heavily on national systems for information, and I think future planning is being designed to continue to use national systems forevermore. As I said to a conference of military officers a couple of days ago, the military is predisposed to underinvest in theater and organic[10] intelligence collection assets: really underinvest big time, because, for a lot of reasons, the services won’t even use the information for operational readiness of their forces. They also feel that there is this tremendous capability available from the national systems.

Student: By theater resources, do you mean things like airplanes and ships that collect?

Allen: Absolutely, or ground-based organic intelligence units. Just look at the budget.

The resultant reliance on national collection is doubled by the development of what we see now as the third generation of weapon systems. We’re getting familiar now with sensor-to-shooter terminology, which comes out of the Pentagon regularly. Now we’re going to have to talk about sensor-to-seeker. Under that concept you’re not necessarily going to have human intervention. It’s going to be the kind of intelligence where you can go from the actual sensor to the weapon itself. I would say that creates an extraordinary change in the way we do business.

I think my role in this is far more relevant than that of the assistant DCI for analysis and production. He works particularly with the national consumer. In my role, because of the use of the national systems, I have to forge more direct alliances with the J-2, with the commands, and with the service acquisition agents. I think the introduction of smart weapons calls into question the assumption that people should do the tasking in the first instance. In the case of third-generation smart weaponry, humans in the loop may put in only noise and delay. As we will see, this may be true for more conventional military operations in the future, because the military is turning to more automated processes that digest large campaign objectives and produce detailed execution orders, such as the air tasking order.

Inherent in these detailed execution orders is that intelligence information needs can be fully developed automatically. This suggests that a meaningful automated interface can be established between operational planning and the intelligence collection systems. I think it’s possible that no single requirements system can capture both the people-oriented national requirements process, which we talked about earlier, and the machine-oriented military processes of the future. It’s a certainty that the current design does not and cannot. We need to review the

[10] The term “organic” refers to functions that are organizationally part of the specific military entity.

compatibility of these two kinds of interactions and develop new comprehensive approaches or a correlated system for these new processes.

Oettinger: Let me quiz you a little bit on something you just said very quickly. Machine-oriented or people-oriented: Is that the customers, or is that the execution systems, or what? Could you spell that out?

Allen: I suppose the national requirement is particularly the people who operate the systems. We operate our systems because doing so requires analysis, it requires that these subjects on which we respond to users be more abstract and intuitive, but when you want information that will help you to sense what's occurring and to send data directly to a weapon, I think you have a different process. I think that's where we're headed. We aren't there yet. It may be years away, but we're moving in that direction.

Oettinger: It sort of scares the hell out of me in this respect, that it also introduces a dichotomy between capabilities and intentions, between the predictable, like a trajectory, and the often unfathomable, like the question of whether I'm going to pull the trigger that will send that thing on its trajectory. If you have an O-O-D-A [observe-orient-decide-act] loop so short that it ignores the intervention of intentions and dichotomizes this world, then it sort of sends shivers up and down my spine. It raises questions of command and control of a degree that nobody, as far as I know, has thought about very much, and whether the results would be sensible or totally chaotic or what.

Student: At a very basic level we have that capability from sensor to actual shooter at the tactical level out there now.

Allen: I believe that in another generation we'll have it from sensor to seeker.

Student: The radar picks up the ballistic flight, senses it, knows where it was shot from, and sends an execution order to the counter-battery to fire on that, and makes the decision?

Oettinger: Right, and the whole thing was a mistake!

Allen: I think technology is pushing it in that direction.

Student: Right now we're still riding herd over it with people, but the capability is there.

Allen: It's still sensor-to-shooter, and will probably be, and in some cases there will always be sensor-to-shooter. I think we're going to find ourselves moving to more automated processes in the way we execute actual battlefield actions. I really do, because everything I see (and I'll defer to the military here) I see moving inevitably in that direction.

Student: You're assuming the guy who pulls the trigger hits the target, and that doesn't happen today. The step right now is that some intelligence source picks the target, but we're not necessarily ready to have the guy pull the trigger.

Allen: We will be. Anyway, that's what my colleagues in the military tell me.

Student: I'm not really comfortable with the idea. You mention the guy in intelligence picks the target, versus...

Allen: Policymakers or whoever.

Student: ...versus the process that we all learned and that the Air Force has developed so well, where you start with a military objective that's really articulated by a warfighter. From the military objective, you decide what the appropriate weapon is and how many of them you need to do a certain amount of damage, and then you figure out the best platform to deliver it. The intelligence guy is in the loop as an advisor, but he's not picking that target.

Student: Half of what I was emphasizing was that the person driving the weapon is not choosing the target. Having the whole infrastructure that chooses the target and how that gets delivered directly to the weapon does not imply that the person is out of the loop with the weapon.

Allen: No, it doesn't mean that, but there is a certain "automaticity" that's going to occur as we develop, and that will require technical information from the sensor directly to a weapon. It might be a counter-battery, radar-directed artillery fire, or it might be an air defense missile bringing down whatever. I believe that we're moving inevitably in that direction.

Oettinger: But it seems to me that there's a doctrinal argument that hasn't even taken place. Let me add another element to it.

Allen: Is that doctrinal argument really going to take place, or is it going to move incrementally, over time?

Student: It's scary.

Allen: I think Tim and his technology are going to drive you in that direction.

Hoechst: You pick the direction; we'll just get you there.

Oettinger: It's worse! With mobile communications, in principle, every grunt in the theater can bring all this apparatus to rain down on the next hill. Are we going to bumble into that?

Allen: It's a risk, but I think there are certain tasks, even for the national community, that will be automatic. They will not be just people oriented. When we have large standing collection decks, for example, in the world of imagery, I think we can probably create a lot more automaticity in that area than we're producing today.

Getting back to the whole question of process, getting back to our ability to do TPED properly, I think we can do a lot of this more automatically than we do today. Now this is provocative, but I think we're moving in that direction.

Hoechst: It is provocative and it's scary. Think about some of the really major U.S. policy disasters in the last couple of decades in such things as shooting down an Iranian airliner or bombing the Chinese embassy, where our processes got broken!

Oettinger: Yes, but there were some significant circumstances in the *Vincennes*, and we've got some documentation right here in the earlier proceedings of this seminar.[11] It was a human error, which might have been avoided had the process been fully automated.

Hoechst: The bombing of the Chinese embassy was certainly a human error as I see it, but, as I sort it out, it was a human error that was driven by not approaching this from the standpoint of military objectives and targets. It was driven by, "We're going to fly a mission; let's fill up the bomb bays, and, by the way, this is the date the missions are going to fly, so you guys had better come up with a whole bunch of targets in a hurry!" It's a backwards targeting system.

Allen: But technology is going to permit us to go sensor-to-seeker.

Oettinger: There's no question that the technology makes a much wider range of choices available than ever before. I'm a firm believer in the fact that we've opened up Pandora's box; in fact, I was one of the openers of the box. That's why I got very concerned over the question of how those choices are exercised, because the notion of technological inexorabilities scares me.

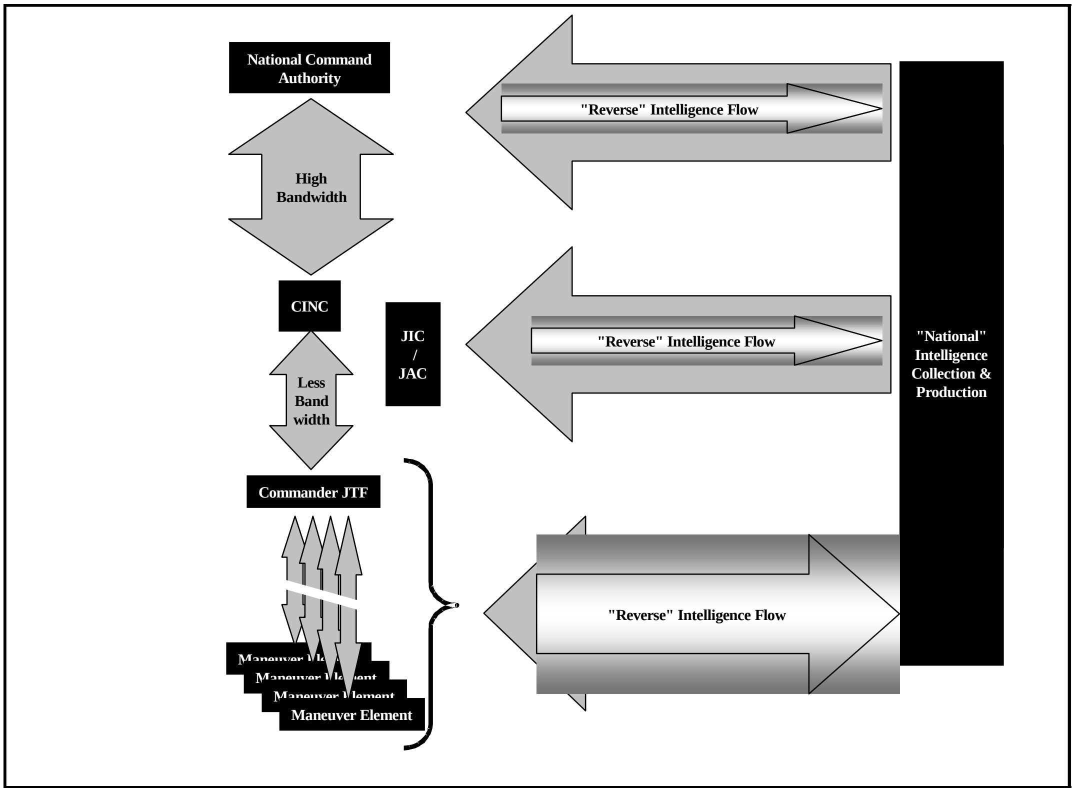
Allen: I'd just like to talk a little bit about one of my favorite areas. In fact, I'm doing some studies for the DCI in this area to try to scope this national-tactical interface. That generally refers to the bidirectional exchange of intelligence information downward from the national collector to theater assets and then upward from theater and tactical collection assets to the national community. There should be some sort of symmetry in the way this occurs. Since Desert Shield/Desert Storm, national collection assets have increasingly been used to support tactical operations, going back to my earlier comment about General Schwarzkopf.

In the pursuit of information dominance, as required by *Joint Vision 2010*,[12] this is both logical and desirable. Satisfying our thirst for a robust flow of intelligence information to tactical forces is going to require a lot of rethinking of our information architecture. For example, the Army has come on-line. It wants more downlinking of a lot of national information to its military units around the world. That's a very fundamental change from where General Schwarzkopf was in August of 1990, when he felt his own organic assets were all that were required for Desert Shield/Desert Storm.

What we have today is this tremendous bandwidth that flows from the national community to the CINC, down to the commander of the joint task force, the JTF (**Figure 4**). There are smaller links down to the military units, to the maneuver elements, or whatever. What I really think should be required, then, is a reverse flow of intelligence back to the national community from theater assets. We can share the two and benefit from the same information. That does not occur in any significant way.

[11] Herres, in *Guest Presentations, Spring 1989* (I-90-3, August 1990); and David S. Alberts, "21st Century National Security Challenges," in *Guest Presentations, Fall 1997* (I-99-2, January 1999); both available [On-line]. URL: http://www.pirp.harvard.edu/pubs.html

[12] Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, 1996), [On-line]. URL: http://www.dtic.mil/jv2010/jvpub.html


National Command Authority
High Bandwidth
CINC
Less Band width
JIC / JAC
Commander JTF
Maneuver Element
Maneuver Element
Maneuver Element
Maneuver Element
"Reverse" Intelligence Flow
"Reverse" Intelligence Flow
"Reverse" Intelligence Flow
"National" Intelligence Collection & Production

Schematic that distinguishes between the chain of C2 and the (optimal) flow of intelligence—the former being hierarchical bi-directional, and of narrower bandwidth at subordinate levels; the latter being asymmetric with high bandwidth "in" at all levels with a proportionately higher bandwidth of information flow "out" from theater and tactical sensors (e.g., UAV imagery) to the "national" intelligence apparat than from, say, the CINC level to the national level.

Figure 4

Student: How do you propose to make it occur?

Allen: I'm posing the question. I don't have the solution at this stage. I'm going to be working on it. I spoke about this to a group of about 300 military people a couple of days ago.

Student: It's not just the military, it's also the State Department, which has collection all over the world learning things and not telling the intelligence people.

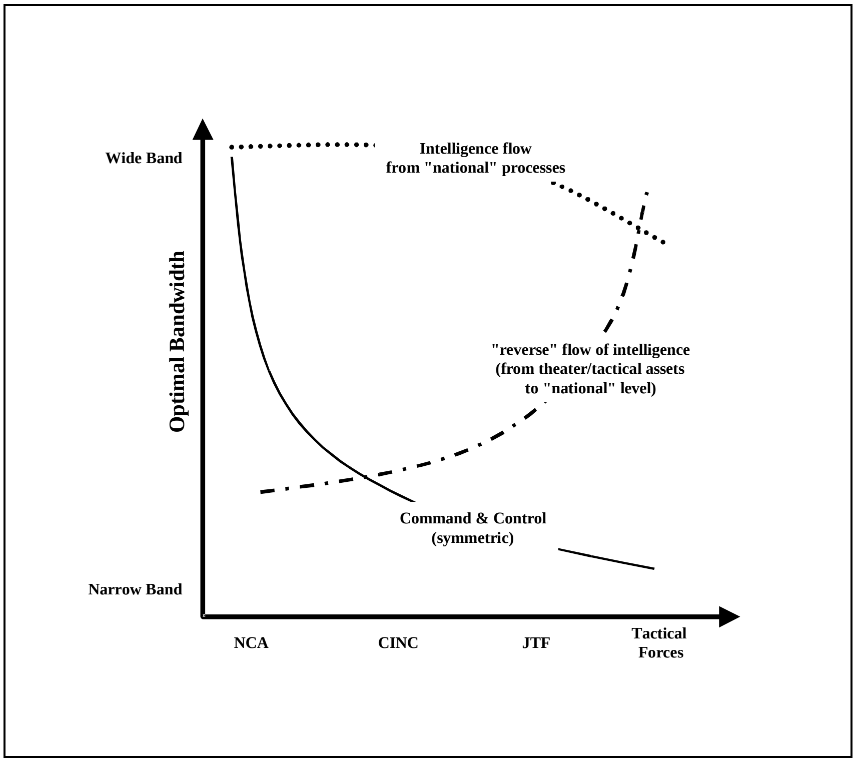
Allen: That's true, but there is a flow of diplomatic traffic that comes around from all the posts in the world. That flows fairly well, certainly to the national community. We get what the embassies think, what their analysis is, and the developments that occur within their own purview. What we're talking about is that there are many organic assets. They may be SIGINT assets, they may be imagery assets, they may fly every day in a particular area of the world, but there's no flow of those data. Those data stay in the theater. In my view, there ought to be some off-loading of national requirements to the theater (where the theater is organic, getting back to General Schwarzkopf's theorem), and let the theater do some things for themselves. But I don't see anything that's changing this. I'd like to see tactical reconnaissance aircraft data made available to the national community. It just does not occur. UAV [unmanned aerial vehicle] imagery is kept in the theater, and there are strong dicta to keep it that way. There is just not this robust flow of information back to the national community. In fact, as I said, I'm doing a study right now that just got started with approval from the DCI.

Oettinger: Jack Leide, General Schwarzkopf's intel guy, gave details on some of that in an earlier seminar.[13]

Allen: Jack Leide is a personal friend. He's a tremendous guy.

This is sort of an objective way things should flow (**Figure 5**). In any event, what we should have is a good flow from the theater back to the national level. The national level clearly has the responsibility to continue its flow to the theater, but we're having some very major shortfalls in

[13] See John A. Leide, "Coalition Warfare and Productive Analysis," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1995* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-96-2, January 1996), [On-line]. URL: http://www.pirp.harvard.edu/pubs.html



Idealized differences between the chain of C2 and the (optimal) flow of intelligence—the former being hierarchical bi-directional, and of narrower bandwidth at subordinate levels, the latter being asymmetric with high bandwidth “in” at all levels with a proportionately higher bandwidth of information flow “out” from theater and tactical sensors (e.g., UAV imagery) to the “national” intelligence apparat than from (say) the CINC level to the national level.

Figure 5

our ability to do strategic national collection because of the continual use of national technical means to support the theater. That is a serious problem. It’s growing in importance to the national community, and we’re going to have to address this seriously and get a better balance. When I talk to senior leaders at the Pentagon, I think they understand that we are going to have to deal with this issue, because the DCI, as you know, will simply not deal with short-term tactical support. He has to work the strategic. He has to work proliferation issues, counterterrorism issues, counternarcotics issues—things that really do require substantial support. I cannot go into them here, but there are issues where we are having shortfalls.

Student: So it’s not necessarily that you want to use what would be sent back, you just want to make sure that you’re not double-tasking assets.

Allen: We’re double-tasking every day.

Student: So you just want to see what we’ve already got out there?

Allen: I think we ought to offload. For example, Central Command [CENTCOM] could offload a lot of its daily tactical requirements. It’s my opinion, but if you’re the J-2 sitting at CENTCOM in Tampa you not simply want the assurance that you’ve covered it with tactical assets. Maybe something has changed, so you also want your national systems to report out the same day. It gives you a level of confidence.

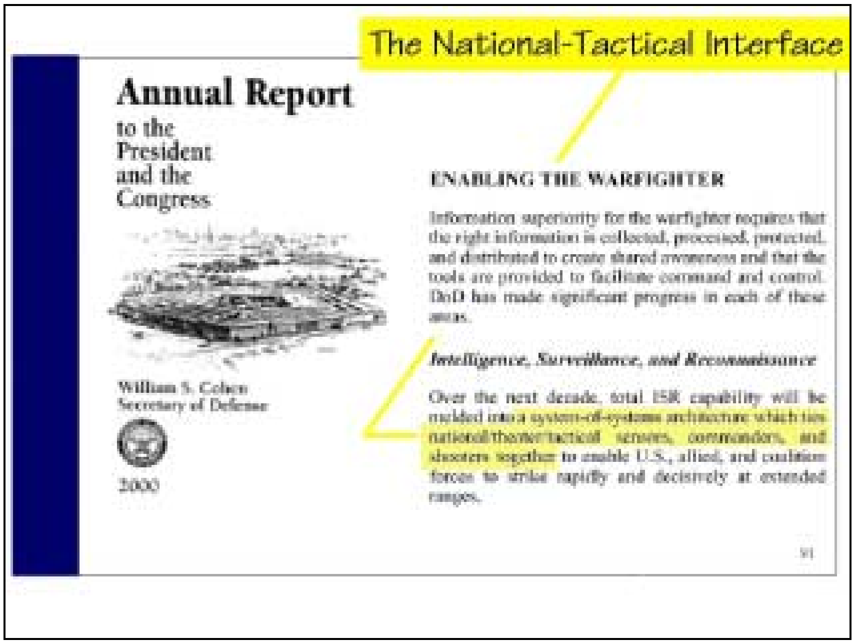
The point is that there is only so much capacity on that national system. There is only so much exploitation capability; there are only so many imagery officers, or SIGINT officers with the ability to report out the information. So, we have a dichotomy here that can no longer be ignored. We’re going to have to address it, and I think the DCI wants to address it.

I’ll stop with this picture (**Figure 6**). Secretary Cohen talks about the need for a “system-of-systems architecture which ties national–theater–tactical sensors, commanders, and shooters together to enable U.S., allied, and coalition forces to strike rapidly and decisively at extended ranges.” I think there’s some recognition of this, but, in my view, we’ve just begun to deal with this question. It’s a big one.

I have other things I could talk about, but I think it’s time for Tim to talk. However, if there are questions that you want to ask, I’ll be happy to speak to them.

Student: Sir, to whatever extent possible, could you address the issue of cooperation between the U.S. intelligence community and the intelligence communities of some of our allies?

Allen: I cannot address that in this forum, except to say that, in all of our endeavors, we have extraordinarily close relationships with friendly governments, allied governments, that support us in many ways to help us deal with national security issues. We could not do certain things without our liaison allies. Counterterrorism, even if it is not a subject of great personal concern to them, is an example. As you know, most, or many, threats of terrorism come against the United States—U.S. facilities and personnel around the world. We have such wonderful relationships with many of our allies that they frequently take significant risks to their own personnel to help us in many areas of the world. But I cannot talk about specific liaison relationships.



The National-Tactical Interface

Annual Report to the President and the Congress

William S. Cohen
Secretary of Defense

2000

ENABLING THE WARFIGHTER

Information superiority for the warfighter requires that the right information is collected, processed, protected, and distributed to create shared awareness and that the tools are provided to facilitate command and control. DoD has made significant progress in each of these areas.

Intelligence, Surveillance, and Reconnaissance

Over the next decade, total ISR capability will be molded into a system-of-systems architecture which ties national/theater/tactical sensors, commanders, and shooters together to enable U.S., allied, and coalition forces to strike rapidly and decisively at extended ranges.

91

Figure 6

Student: Can you mention at which level most of these relationships take place? Do they happen at the DCI level, or do they happen elsewhere?

Allen: They happen frequently at the DCI level, but they also happen at working levels on a day-to-day basis worldwide. They're very rich and very robust, and Director Tenet has worked very hard around the world to increase our liaison relationships.

Student: I'm not familiar with I&W, indications and warning intelligence, as I've never been an I&W analyst, but I've been around it. As you've described it, it seems to be one dimensional, or, as a matter of fact, even less. There's one degree of freedom. You're looking at events and the question is: Will something happen, or will it not happen? The output is usually a one or a zero. A lot of events we're looking at could have many possible outcomes. How does I&W play into that when you've got a number of different dimensions, or a number of different degrees of freedom in which things can go?

Allen: To a warning officer, the glass is always half empty, it's never half full. You're looking at issues before the policy community tends to pick them up. When I was an NIO, my staff and I continued to look at indications of developments. You're right. Sometimes we don't know exactly if an event is going to occur once we start seeing signs that bother us, which probably do not bother the desk analyst—the all-source analyst who handles it geographically. We found those people were probably the last people at times to recognize an abrupt discontinuity. So, we actually work alternative hypotheses.

I think that the secret of warning intelligence is not only having bright men and women to help you but also to work methodically: to use rigor in the way you do things, not just to build an indicator list, which we did, but to build templates of how this country has behaved in the past. We've done this, with great rigor and with great success in some cases. In other cases, we did not.

In fact, when the warning officer is doing his job best is when the policymaker, or the Congress, hardly notices it. I remember briefing Congressman [Steven] Solarz,[14] an extraordinarily bright man, to whom I described a crisis that occurred on the Subcontinent in 1990 in winter and spring and how we gave warnings repeatedly when the warning community, the all-source analysts, could not recognize there was a problem. Then, by the spring of 1990, the all-source analysts were more alarmed than we in warning were. Earlier they were totally scornful. But in those cases, we had skillful diplomacy: we had Richard Haas [staff director for Near East/South Asian affairs, NSC]; we had Bob Gates [then deputy national security advisor], and we had John Kelly [assistant secretary of state for Near East/South Asian affairs]. They defused a crisis on the subcontinent through diplomacy, intelligence, and extraordinary support. The reason Bob Gates and John Kelly and Richard Haas were there is because we had excellent warning.

I explained all this to Congressman Solarz, and he said, "Well, gee, we never knew intelligence and warning played any role at all in that process. We thought that was just a great triumph of diplomacy." But that was when under Judge Webster, and under the community, we had extraordinary intelligence. Two countries were getting into a state where I think they could have actually engaged in conflict. But we look at all those complexities and we develop separate options and alternative hypotheses.

I frankly am not very comfortable with the warning community today in Washington or the way it does its business. I don't know whether you've had Mary McCarthy up to speak here, but she's the director of intelligence programs. She was the NIO for several years. She was my deputy for three years as the NIO for warning. She brings the same kinds of strong views I do on the warning community and the need for extraordinary rigor. I refer you to articles that Mary McCarthy and I wrote for the *Defense Intelligence Journal* in June 1998.[15] You get the *Defense Intelligence Journal* here at Harvard. It's an unclassified journal. I wrote an article on how we warned on Iraq—which I enjoyed writing, by the way—and Mary McCarthy wrote about the extraordinary need for more rigor and methodology in the warning.

Student: Do you employ red cells as an analytical technique?

Allen: Absolutely. I'm no longer the NIO for warning, although I keep an eye on it. One took place after the explosion in the Thar Desert in May 1998, which was a very disturbing event where warning was not very good and where all-source analysis was not good and collection was not good. Admiral David Jeremiah, a brilliant American, wrote the critique in three weeks' time—a review of what was wrong.[16] The one thing that really struck him, and he's talked to me about it numerous times, was the lack of red teaming, the lack of alternative hypotheses, and the lack of rigor with which the community approached these issues. Now, under John McLaughlin, who is the deputy director of intelligence, and under John Gannon, who is assistant DCI for analysis and production as well as chairman of the National Intelligence Council, a lot of that is

[14] Dem.–N.Y.

[15] Mary O. McCarthy, "The Mission to Warn: Disaster Looms," *Defense Intelligence Journal* **7**, 2 (Fall 1998), 17–31; Charles E. Allen, "Warning and Iraq's Invasion of Kuwait," ibid., 33–44.

[16] Admiral David E. Jeremiah, USN (Ret.), then acting director of the National Reconnaissance Office.

going on today, and good results are being produced. We really do need that kind of thinking, that kind of rigor in the way we do things.

You're right in raising the issue of red teaming. This has not been a forte of the U.S. intelligence community, and it should be. When Bob Bowie served as director of the National Foreign Assessment Center, he was essentially the deputy director of intelligence, and he also was chairman of the National Intelligence Council.[17] I worked directly for Dr. Bowie, who, I guess, was emeritus at Harvard. One thing really bothered him when he came in: the lack of alternative hypotheses. He even put out a classified journal under his aegis where he encouraged analysts to publish their thoughts, to put down what worried them: alternative views or "here is the book solution." He encouraged them. After he left, that journal disappeared. So, we have a penchant not to engage in this kind of debate and dialogue.

I enjoy it. I think we should do it all the time, and we're doing better. George Tenet is ensuring we do it, as are John McLaughlin and John Gannon. We have a long way to go to do it in the way we should. I think our warning community needs further strengthening in Washington.

Student: About a month ago there was an outcry in Europe about the allegations that the United States and the U.K. used the information collected from the military suppliers for the European Commission...

Allen: …for the advantage of U.S. firms? That's absolutely false. The U.S. intelligence community does not collect economic intelligence to support Lockheed Martin over Airbus Industrie, or Boeing over Airbus, or anyone else. I think if you want to read anyone about that, read the op-ed piece by Jim Woolsey that appeared a few weeks ago in the *Wall Street Journal*. The U.S. intelligence community really does have responsibility to the policy level, not to any private sector or firm. We give no assistance to the private sector. One of the vigorous things that is good about this country is that we don't do that.

Oettinger: The rumor was probably spread by the French.

Allen: But if there are corrupt practices, as Jim Woolsey always said, we want to keep the playing field level. I believe that General Dynamics and General Electric and Lockheed and others should have the right to compete internationally on an even basis. If there are corrupt practices or bribery is heavily involved, and there's information that tells you that bribery is involved, we don't assist the private firm but we certainly send our diplomats to protest to the government involved. We're also working internationally, of course, to get better conventions that will prevent these kinds of corrupt practices, which are very prevalent in the world. As Tim knows, the penalties in this country for a private sector firm that engages in this kind of corrupt practice are extraordinarily heavy, and it works. In this country, we go out and compete fairly.

Oettinger: Sir, this has been an absolutely marvelous short course, I might say, in the full range of intelligence activities. I can think of no reading that was assigned this semester, or that I could

[17] Robert R. Bowie, professor of government and international affairs, Harvard University, directed the National Foreign Assessment Center from October 1977 to August 1979.

have conceived of, that would have given the same scope of coverage in so neat a capsule as what you heard here today. We’re very grateful to you. Here is a small token of our appreciation.

Allen: Thank you very much.

Oettinger: Now, we’re very fortunate in that both gentlemen will be around, and as Tim commented on Charlie’s presentation, it will be vice versa.

Acronyms

ADCI	assistant director of central intelligence
C2	command and control
CENTCOM	U.S. Central Command
CIA	Central Intelligence Agency
CINC	commander in chief
COSPO	Community Open Source Program
DCI	director of central intelligence
FBIS	Foreign Broadcast Information Service
HUMINT	human intelligence
I&W	indications and warning
JROC	Joint Requirements Oversight Council
NIO	national intelligence officer
NSC	National Security Council
TPED	tasking, processing, explitation, and dissemination

INCSEMINAR2000

ISBN 1-879716-74-7