INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Shaping the Intelligence Environment in the Information Age
Kenneth A. Minihan

Guest Presentations, Fall 1997
Jr. Robert R. Rankine; Victor A. DeMarines; Keith R. Hall; William R. Clontz; Kenneth A. Minihan; Henry A. Lichstein; John J. Sheehan

January 1999

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.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-54-2 **I-99-2**

Shaping the Intelligence Environment in the Information Age

Kenneth A. Minihan

On 23 February 1996, Lieutenant General Kenneth A. Minihan, USAF, was appointed the 14th director of the National Security Agency (NSA)/Central Security Service. In this capacity, he is the senior uniformed intelligence officer in the Department of Defense. Immediately prior to this appointment, General Minihan served as the 11th director of the Defense Intelligence Agency, Washington, D.C., and director of the General Defense Intelligence Program. During his career, he has commanded several squadrons and groups in the United States and overseas. He has also served in senior staff officer positions in the Pentagon, Headquarters Tactical Air Command, Electronic Security Command, and NSA. In Vietnam, he served as a target intelligence officer and command briefer for Headquarters 7th Air Force, Tan Son Nhut Air Base, near Saigon. He entered the Air Force in 1966 as a distinguished graduate of the Florida State University Reserve Officer Training Corps program with a B.A. in political science; in 1979, he earned an M.A. in national security affairs from the Naval Postgraduate School; in 1993 he participated in the Kennedy School's Program for Senior Executives in National and International Security. Among his awards and decorations are the Defense Distinguished Service Medal, the Legion of Merit with two oak leaf clusters, the Bronze Star, the Defense Meritorious Service Medal, and the Meritorious Service Medal with three oak leaf clusters.

Oettinger: It's a particular pleasure to welcome General Minihan for two special reasons. One is that he is an alumnus of the school, so it's nice to welcome him back. The second is that I've had the pleasure of working with him in other contexts, particularly during his stay as director of DIA, and learned to appreciate his thinking and his wit. And so, it's a real pleasure, on that ground, to have a chance to hear him again. He has indicated that he has some thoughts to present, but he welcomes questions as they arise. I trust you will be your usual nonshy selves, and ask questions as they come along. So saying, it's all yours, sir.

Minihan: Great. Thanks very much. We're delighted to be here. If you're from Washington, D.C., you're pretty easy to please if you can get out of D.C. and spend some time away.

I took as my homework assignment to have some discussion with regard to intelligence and command and control as you're looking at them. I'm going to contrast where I think we are today with where I think things will go fairly quickly. I'll lay some huge signposts out as we go through that. Then we can take the discussion anyplace you want to.

When I'm in sessions like this, I always begin by saying that my generation was raised on Clausewitz. We had to read it. I know which parts you're supposed to quote. I think, essentially, you're leaving the Clausewitzian world and you're entering the non-Clausewitzian world, particularly if you are interested in studying, being a part of, or practicing intelligence in the context that we do today. It's very important that you recognize the switch from Clausewitz. I'll come back to that thought in a moment. But if you look at the F-16 shootdown over Bosnia a couple of years ago,[1] that is so non-Clausewitzian that it's beyond your mental capacity as an intelligence officer to have thought your way through to understanding how they would have been able to track that airplane and shoot it down in the context that they did.

I believe, then, that for the moment technology—not doctrine—is the applicable element to watch, and that technology will drive

[1] The Scott O'Grady incident in 1995.

the business of intelligence whether you're a policy maker, a military person, or actually in combat. So, for at least this period of time, technology is going to be the key component to shape change.

I want to review three important changes. Historically, in the intelligence field and for command and control, we have tried to describe what was going on in as near real time as we could. I think the business of the future will be to shape the environment in which we'll operate, which will be less interesting as a postscript or description, but more interesting in the context of what kind of an environment you would like to operate in. The American and allied "lesson learned" for that is Desert Storm. The way you achieve the maximum potential for things you want to do is in a shaped information environment, and Desert Storm was a good example of that. We can pursue that if you want to.

Secondly, we'll move to a much friendlier display of information. So the high ground is going to be full access to any information you want, as opposed to the historical limitations on quantity and access and so on and so forth. I think, by and large, we'll have a fairly massive set of information.

Lastly, if you're studying this business, you will find in all of your readings the term "support." That term is intended to characterize what intelligence and command and control have done in the past, which is: support the policy maker, support military operations, support law enforcement. You'll see that word a lot. I think that word will change to "participate in," and that what you will find, if you were to choose to join this business, is that you'll be inextricably tied to success or directly involved in failure, as opposed to the historical supporting parameters. So, we will elevate the state of play of the business of the study, practice, and examination of intelligence relative to shaping that environment, which is richly filled with information, and which is very high tech. In my view, it's become a tough, complex business, sometimes dangerous and life threatening, and that will be the nature of it in the 21st century.

The question, then, as you study it today, is how it can stay relevant to the interests of the nation, as the interests of the nation move from the industrial age to what I'm going to term the "information age," for lack of a better phrase. I want to use "information age," because what I'm going to suggest to you is that the terms you hear now—"information warfare," "information operations," and all that—are much too limiting. What most democracies are really looking at, as they enter the 21st century, is "conflict in the information age." That conflict will be characterized by an entirely different set of characteristics, and I'll go through those in a second.

Conflict in the industrial age was characterized, by and large, as a physical relationship, and there were these notions of geopolitical centers of gravity. In the United States that was the industrial base. If that was the strategic sanctuary of the 20th century, then as we develop our information technologies and we become the complex nations of the 21st century, what does the strategic sanctuary look like for us? All of our generations have always understood what that sanctuary was and protected it, so that you could conduct the democratic business of the government, protect the citizenry, and succeed economically; so that Harvard could exist for hundreds of years and you all could come here to study; and we could have all the things which we're accustomed to.

Now, my friends in the United Kingdom, when I talk like that, say, "Strategic sanctuary is a uniquely American concept. It is not necessarily a thought that is international in its context." So it does conjure up a notion that Americans have strategic interests around the world, which may not now be located in the United States. That's a completely different strategic concept than the one we protected in the 20th century. If that's the case, then the information infrastructure that we're building is no less important to us than the industrial infrastructure of the 20th century was. The change is in the strategic coin by which we judge that infrastructure and its "globalness," as opposed to its isolation on fortress America.

I shared with some folks who were here during lunch that, if you look back, essentially all of the keels that the Americans floated to win World War II were laid in the 1930s. The question then is, relative to the information age, what do the "keels" look like that we need to invest in for the 21st

century so we can secure that same prosperity? I think it's an important issue.

I'm going to use the term "superiority" to clearly set in mind here that there's a relationship, and that relationship is dynamic. Superiority suggests it can wax and wane. It can be changed by different dynamics. It is not "My pile is bigger than your pile, and that's the end of it." So now intelligence clearly enters a domain where, if superiority is used, it isn't just a function of your ability to collect information and give it to customers and so on, but it's the quality, the quantity, and the degree relative to what your adversary has. That relationship changes every day in all of the complex ways you can think of. There is not a steady state of "Your strategic sanctuary is secure, your adversary's is not, and you've achieved a superior relationship." If you've become participative, it's something that you have to integrate with the everyday operations of the nation and the nation's allies.

So whether you're a policy maker, or in the military, or in industry, maintaining that superior relationship in that technological context, given all of the cross functions that we have to have—nation-to-nation relations and so on—is something that we will have to attend to every day. That is much different from the way intelligence has been thought of up to this point. It becomes a daily need for our consumers—our leadership. Industry needs it daily, and our allies need it daily.

So the trend in that strategic line suggests, in my view, that you are in a revolution. I'm okay with the notions that there is a significant change occurring here, that technology is the wave we want to ride for a while, and that we don't want to dwell on doctrine and things like that for the moment. Most leading democracies, when they reach these conditions, are excellent at opening up a very rich academic discussion of what our vulnerabilities are; what our opportunities are; what our shared interests are; how that all should be mixed in such a way that we, as democratic nations, succeed; and then finding the kinds of solutions around which we can develop a consensus.

In the industrial age, those strategies allowed us to secure the Cold War, to develop civil defense so we understood how to defend the nation's industrial base, and to develop a consensus with regard to investment in national security and law enforcement. Those are the same conditions that will be necessary if we're going to have the same rich heritage in the 21st century. I like Toffler[2] a little bit, in the sense that there is some context for you to deal with this revolution beyond what you will normally hear described as a Revolution in Military Affairs. I think you have to deal with it at a somewhat higher level.

If I could use computers as an example, computers derive from the mid-to-late vestiges of World War II, when we were unable to break codes without our ability mathematically to exhaust options found in the codes. Computers resulted in the United States' breaking both the Enigma and the Purple codes. The breaking of those two codes allowed us to know what the Germans were doing, and took us through to what was a shortening of that combat. If you were to look at one of those old computers today, it's as long as this table and had really no capability.

Those computers, then, became the PCs. But you all have moved beyond that. I remember when you had a computer on your desk, but it wasn't thought that I would connect to your computer. My computer helped *me*. It didn't have anything to do with our interpersonal relations. We're moving from the PC-centric to a network-centric environment, where we hook our computers together, and we begin to develop an infrastructure that looks a lot like the industrial age, but it's virtual. So we begin to develop the capability to take advantage of our computers and use this new emerging information technology that we're investing in. That will lead to a content-centric environment, where the computers will have, resident in this virtual environment, the data that we would then call "knowledge," and that we need to carry out electronic commerce, banking, personal relationships, and so on and so forth.

So if there are things occurring, it isn't the first wave, second wave, third wave. These waves are rolling together. Some of us

---

[2] Alvin Toffler, *The Third Wave*. New York: Morrow, 1980; Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little, Brown, 1993.

are in PCs, some of us are in networks, and some of us are in content, and we're moving through those. As democracies in the 21st century, our ability to use those is contingent on intelligence being able to provide an operating environment in which we can trust the use and deal with the misuse just as, in the industrial age, you could trust the use of electricity, and telephones, and all the things you are accustomed to, and deal with the misuse.

If I could use the information highway as an example, we need to be confident that people on the information highway have licenses, that we know how to arrest speeders, and that we can find and deal with people who use the highway inappropriately, just as we can, physically, deal with someone using our highway structures now. We need to be sure that, other than a few countries in the world, we all drive on the same side of the road. (My apologies to those of you from the U.K; I didn't mean to say that.) So, you have some shared international relations there.

Now, if that's the case, then one has to ask a question, "Is there a threat to that prosperity?" In other words, in the United States we're investing $1 trillion a year in our information technology. Is there a threat to that investment that would cause us to think about the security keels we need? Let me talk about that.

There are two major trends that occur. One is in the nation state area. The threats there tend to be what you all kind of think about as the number of states that, like Somalia, just simply dissolve on us and cause us to deal with completely different cultural conditions than we've had to deal with in the past. At the same time, there are rogue states, such as Iran, Iraq, and North Korea, that threaten regional stability, in which we all have strategic interests.

What you see now is a trend, and I'm just going to say for a moment that by and large the nation states' geopolitical power and centers of gravity are diminishing. There is a concurrent rise in the center of gravity in the power of transnational threats, such as terrorism, narcotics, worldwide crime, criminal cartels, and so on. So, you have this concurrent rise in transnational power and a diminishing of the nation state, and in that context a loss of geographic confines as the way we do our normal business. The new technology now has intertwined our borders and our boundaries in such a way that these things can't occur around the world without there being some disruption. That disruption then causes us to have mutual interests in security, law enforcement, and commercial activity.

The second part of the threat is that we fielded a network in which we have essentially no security services. For the most part, major industrialized, 21st century nations have invested in their information infrastructure in such a way that it's vulnerable, and the way we want to do our business is vulnerable to disruption. So we now have what I would describe as asymmetries between our vulnerabilities. Our vulnerabilities are not necessarily only physical anymore, in contrast to some of our adversaries' vulnerabilities, which still tend to be that way. Absent having some security environment in which we can protect our networks, they're vulnerable to exploitation and disruption. So, it is not inappropriate to worry about an electronic Pearl Harbor just as the generations in the 1930s worried about an industrial age Pearl Harbor. It's not inappropriate to discuss your security concerns here.

Oettinger: This may be picking a nit, so stop me if that's what I'm doing, but you're talking about physical versus nonphysical as if electronic systems were not also grounded in physical reality. I don't know how to muck around with data except that the data is somewhere and I do something to it. It takes less energy than to knock off a bridge, but I still have to do something on some tangible thing that requires energy.

Minihan: It's an excellent point. The point I mean to make when I say "virtual" in that sense is that the vulnerability of the bridge can be seen in its physical location. The vulnerability of the network is not seen relative to that. If the telecommunication switch is in Brooklyn, its vulnerability can be outside the United States, and so, it's not secure in the context that it's in Brooklyn.

Student: We can all imagine vulnerabilities and threats to certain systems, but how likely are these threats? Do we have any evidence

that these vulnerabilities are going to be exploited by terrorist groups?

Minihan: We do. Let me give you sort of a collective view. First, as an evidential base, the U.S. Department of Defense experiences nearly 400 computer penetrations annually. The U.S. Social Security Administration tried to put its files online, but had to withdraw them because people were manipulating the data stored in the files. The most recent one I saw was that a guy who tried to offer credit rating support had to withdraw.

You all surf the net just like I do, and if you look at the hacker side of that, that's what I would describe as the tip of the iceberg with regard to what one can do if one doesn't care about being caught. For most hackers, the thrill is, "I did it." They want you to know they did it. What you don't see is the part of the iceberg that is what's going on now that you don't know about, but you have a lot of evidence to indicate it must be relatively important because there are hackers there, and there are lots of penetrations. Every time somebody's tried putting up sensitive information they've had to withdraw because they've been exploited.

The other commercial aspects are in what I would describe as our banking and telephony industries, where you see the loss of money in electronic transfers. If I use my cell phone in New York, somebody will steal the number on me. You see a lot of evidence of commercial misuse.

Then lastly, for the most part there is an array of nation states that see the strategic context that we're discussing, and just like the United States, and just like the countries some of you come from, are now having very rich debates about two aspects. One is, "How do I take advantage of this as an offensive capability?" In the United States, we're now talking about, "What are my defensive responses? What does information assurance mean?" So there's a rich set of data out there to indicate it's a widely used approach.

Student: These threats are fairly different in nature. The criminal threat is always going to be there. There are always going to be people who are going to seek to exploit the latest device to try and move funds electronically. What I'm more concerned about is how likely you think the threat is of, firstly, an agent or some other group trying to get at this nation's security information, and, secondly, a terrorist threat. For example, over lunch you were mentioning toxic waste on a train, and someone trying to intercept information in order to produce a catastrophe of that sort. There must be different threat assessments for those sorts of things.

Minihan: I kind of meant to sweep those up. I don't know what you mean by "likely." My view is that they are likely. If you mean, can I go and point to a terrorist, what I'm telling you is that among the computer penetrations that we see, they're not all hackers. Remember what I told you: the difference between a hacker and a terrorist and a nation state is that a hacker wants to be caught and a terrorist and a nation state don't. If you have no security apparatus in the network, then you have no way of knowing what's going on in there, and that's why I use the tip of the iceberg as an example. We don't have a regime of detection and reporting that lets any of us know what's going on. That's why it causes the second debate, which is: What security regime should we put into our network environment so we have some security services in there and we can trust it?

Student: I think what I was asking was how you would prioritize these threats. If you were given a budget tomorrow, where would you spend the money? Which particular threat would you be most concerned about?

Minihan: Because of the way I'm dressed, I'm most concerned about the threats to the nation's strategic sanctuary. If I were a banker, I'd be most concerned about my commercial vulnerability. If I were working for the FBI, I'd be worried about domestic law enforcement. I think you have a shared set of concerns.

My attempt here was to say that's exactly what they faced in the middle of the 20th century. They had shared vulnerabilities—the industrial base, the national security, and law enforcement—and they needed consensus for a wide-ranging strategy. I used the example

of civil defense, because in that strategy there were federal, state, and local responsibilities. I'm old enough to remember that when they set the siren off, we knew how to get under this table. Nobody said, "This is stupid! We're not doing it!" We all thought that was an important thing to do.

We need the same consensus to emerge. As we were discussing this at lunch, I agreed with Professor Oettinger that we are going to have to spend some time discussing and studying it in order to get the same consensus. And remember: now it can't be just an American solution. Now it's got to have more dimensions.

The asymmetries between the vulnerabilities are kind of an interesting thought, because from a national security perspective, a law enforcement perspective, and a commercial perspective we're accustomed to symmetrical competition. What do you do if you field the larger combat power, but the adversary chooses to respond in the information domain, in an environment where your telecommunications infrastructure is at risk? You say, "No. No. I want to meet you on the field of battle." They say, "We understand you're going to win that. That's not where your vulnerabilities are. So we're going to attack your strategic sanctuary, not your center of gravity."

The asymmetric relationship, then, deals with the issue of shaping. How do we shape the environment so that we can recognize those asymmetries, be able to operate in them, and at same time protect what may be our strategic sanctuary? In this case, it might be separated from the field of play. So I think we play chess, not checkers.

Oettinger: Could you help me distinguish between what you mean by "center of gravity" and "strategic sanctuary?" I can't construct something out of this.

Minihan: I'm pursuing the same thought we did over the bridge. Clausewitz would only have centers of gravity. A strategic sanctuary can be characterized uniquely as virtual and physical. It doesn't have to be only a center of gravity. Our sanctuary may well turn out to include elements outside the physical confines of the United States, whereas our center of gravity was historically thought of as the continental U.S. We even used that phrase in the industrial age. Every business, every military, every house can have a center of gravity. But if you look at its strategic sanctuary, my house could be connected to your house, which is a completely different relationship.

I now want to switch and say a few words about intelligence. If you look at conflict in the information age, then you have to ask yourself in the traditional sense, "What does intelligence look like to me, as I go around the turn of the century, and I start talking about being relevant to the nation's interests?"

It is very difficult to envision. I'm going to use three examples. We can go through a bunch of them. First, let's talk about how you would do analysis. You would begin to do analysis based on infrastructure; not based on air order of battle, ground order of battle, or political things. What you'd like to see is your adversary's infrastructure so that you see their technology template, not just their geopolitical "here is what my country looks like" and so on and so forth. I'd also let you see transnational actors, because transnational actors are now in the seams of the way we think about things. Dr. Oettinger knows that in DIA we had the Russian shop and we had the whatever shop, and in there there's an air order of battle analyst and there's a political analyst. We will completely shift the way we do our analysis.

The second thing is that if you look at infrastructure, then you're going to want to know what the technology looks like in the infrastructure, and you want to know cultural use. You want to know a lot of things about that because you want to shape it. You want to understand how to deal with it because you'll be having this constant exchange of dynamics as opposed to the relatively unusual conflicts in the industrial age of combat. In a sense, the idea of peace is dismissed, and you're always in competition. The question is whether that competition moves to conflict and war as you move up and down in it. What you want to do is try to keep moving yourself, keep yourself in the competition phase for as long as you can, and only go to conflict or war when it's shaped, and it suits you to operate in it. So, analytically, we'll

look at infrastructure, and we'll use technology templates.

We're also going to require a huge amount of information to do that. Therefore, the second big impact is that we will have more information than we can possibly imagine. We won't, as we've done in the 20th century, seek the lowest common denominator and diminish our information storage. So we'll have to look at very intense intelligence operations, intense use of technologies for storage and retrieval, and then, a very agile context of how we present that to our customers because they will now have access to this huge amount of data.

And then, lastly, as I mentioned in the beginning, if you're inextricably tied to success, then you are participating, not supporting, and the phrase that will be used in that context will be "integrated." Intelligence will be fully integrated into the policy maker's regime, into the national security regime, and (I'm going to argue) into the commercial regime of the future, so that we share the sense of threats and vulnerabilities much more broadly than was necessary in the 20th century, because the industrial base was not at risk as long as we could protect the continental United States. That says that we need a national strategy that has international components. In that strategy, we need to be able to protect the strategic sanctuary, and in that sense, it must be defined in some way so that we begin to understand our global partnerships.

The intelligence responsibilities in that are really interesting. What are indications and warning (I&W) of a cyber attack? If we analyze infrastructures and want to understand how telecommunications and information communications technology react, then we have a lot of studying to do if we want to perform the normal business of understanding what's going on and how we present warning. If we were to be able to do that, then how do we do attack assessment, and how do we determine our normal responses to it, since it's asynchronous and has all of the other characteristics of playing chess? Some of the pieces won't move in a straight line, others are going to be more powerful, and so on and so forth. That matchup may not take place on the battlefield as we had hoped, but it's somewhere out there in cyberspace.

So you have the complexities of doing attack assessment for response. Gone forever is the smoking gun—the 20th century's "I can prove you did it." Now, the policy maker and the intelligence analyst have a huge challenge, because you have operations going on where the democratic test of proof, the smoking gun, won't exist. The policy maker will have to make decisions based on accountability and response, without a solid lawyer sitting next to him saying, "Yes, internationally, this will meet a juridical test that would allow us to pin the full blame for this on ... (you pick it). We know where the attack came from." We won't know those kinds of things.

So now, the associations become much more complex, and, in the context of holding entities accountable, whether they're transnational or nation states, will be very difficult for the policy maker. Right now, the United States is the nation that brings the greatest vulnerability into play for this.

Oettinger: Can I try to pinpoint your views? Again, why is this different from a Wild West where anybody can tote a gun, and it's not registered. Bullets are reported in somebody's backyard; somebody shoots somebody, they've got a hole in the head, and you say, "Oh, *he* did it!" Who knows? Now you have another environment in which guns are registered and the bullets are manufactured in a number of places, you can trace the bullet, et cetera. Your ordinary household spouse murderer is usually tracked down, although occasionally there is somebody really clever or terribly stupid, and you can't figure it out. But why are bits not as traceable as bullets? We have a Wild West situation now, but I can imagine that, for a certain transaction cost, which is getting smaller and smaller, and a little bit of politics, every damn packet can be registered in some way, so that you can't get a packet on anything without its being infinitely traceable.

Minihan: Tony, you make two excellent points. Let me agree with the first and not agree with the second.

First, I think you correctly characterized today's network, in the sense that there is no accountability. There are no security services.

It's like a party line. I would make the argument that people can, with some impunity, masquerade. It's a normal technique used by hackers, and you would not be able to trace the bits to bits. You could make an argument that with a solid set of keels in there for security services you could diminish their ability to do that. For example, if in order for the two of us to conduct any sort of business on the Internet you had an electronic signature that you had to sign, just as you have to sign your check, it would be much more difficult for you to masquerade. So there are opportunities for us to deal with it in the future.

I was telling the folks at lunch that it's really interesting to watch how people act on the Internet, distinct from the way we act when we're looking at each other. You have that exact same set of characteristics in a much more fundamental strategic sense when you start looking at the Internet as a network environment.

I was using the analogy of the information highway—having licenses and things like that. If we're going to conduct business, we don't see each other. Right? When I'm hooked up, how do I know that just because I'm looking at his e-mail, that's Oettinger? If it is Oettinger, how do I know that what Oettinger is saying to me is what he's actually sending? So I want to know who you are and that the information I'm receiving from you is correct. Once we've completed that transaction, I'd like to know that it's finished. When you say good-bye, I want you back out of my system. Then, when we've completed that, if I want to talk again, I'd like to reestablish that assurance. Those are basic things that we're accustomed to in our industrial context that would then, I think, deal with some of the problems. But absent those, the digits can masquerade.

If you guys do your Saturday morning scenarios here, one of the things that's really fun is to have somebody like me come and say, "Since Iran practices information warfare, I think they're responsible. Since I'm in the military I want to go bomb them, because their vulnerability isn't in their information infrastructure, it's in their physical infrastructure. Let's hold them responsible anyway, and let the policy maker deal with it."

Student: You talk about this from the U.S.-- perspective in terms of a defensive capability. The U.S. military has operational plans to deal with certain contingencies all over the world. Do our current or future operational plans include components to deal with cyber warfare and ways to attack and defend?

Minihan: Yes, as you'd expect, they now have a section that deals with both protecting and attacking. Remember what I told you: the plan connotes a vaccination, in my view. If you look at planning from a military perspective in the Cold War (I'll pick the central region scenario), the intention there was that if the Soviets came across the central region, we had an O-plan (operations plan) that vaccinated us against that scenario. We said we had a force structure on it.

What I'm taking away from you is the peaceful phase of that. So, what I'm saying, – in effect, is that you can build an O-plan, but you have to tend to it every day, whereas historically we could build an O-plan and we could say, "We have the ability to do it. Let's practice it once a year, or once every two years, just to be sure, and then that can sit on the shelf and is sufficient." I think that peaceful phase, where we're not in conflict, goes away and is replaced by a competitive relationship, which is much less amenable to being managed in a plan. But it still is the case that it'll be in plans.

Oettinger: You've clarified something. It seems to me that may be something that is more poignant for the military than it is to the rest of us, except, perhaps, the police. In a sense, every day I'm concerned as a householder about things that I might do that might invite robbery, and every day I'm concerned about taking some measures to protect myself against it. The police are out there every day, and yet people still get robbed, although by and large they don't. So it may be that, if I hear you correctly, you're sort of saying that the situation is more like a continuous policing than a spasmodic military campaign.

Minihan: I meant it to be continuous policing, continuous military, and continuous commercial. It's the environment in which we're going to live. Robbing your house may

no longer equal entering your house; attacking our nation may not equal bombing a bridge; and commercial espionage may not equal breaking in and stealing products. It may be your intellectual property.

Try this on for size. If I took Microsoft and General Motors and made them about the same in terms of their net value, and then I sold off all the physical assets of General Motors and I sold off all the physical assets of Microsoft, but I kept the people on both sides, where have I got a big investment? In Microsoft, right? Over half of Microsoft's value is in the intellectual property of its people. In that sense, they have a huge interest in protecting a commodity, which we don't have.

Student: That's if you want to do software. If you want to build cars you'd rather have the GM employees. They have intellectual property also: each of them has a unique set. I would say that, given the unique set of data that each maintains, the larger the organization, the less likely it is that data structure will change over time, because it's big. While we have to do constant policing, and the time scale will shrink from two-year O-plans to one-month O-plans, you still shouldn't expect the turbulence that I think many predict when they say, "People are going to change their data structures, and we can't make a plan because it will always change." It doesn't change very fast. It changes faster than building a fleet or building any army does, but it doesn't change on a monthly basis, or else the commercial, the military, and intelligence organizations wouldn't be able to do business.

Minihan: What I said was the environment in which the O-plan will be introduced will change. So, I think you and I can agree. I wouldn't characterize the O-plan as changing moment by moment, but the environment in which I submit the O-plan will be changing.

Student: The I&W for it is very, very difficult. It can be responsive instead of preemptive.

Minihan: Yes. "Shaped" is the term I use for it.

Now I want to introduce one more term—"simultaneous"—into the intelligence discussion. In an intellectual context, one would expect people who understand intelligence in the 21st century to get the point that the same information can be in several places at the same time. Simultaneity should become a concept that we're comfortable with and that we understand relative to the way we will collect, analyze, and report. To go back to this discussion we just had, if that's the case, and I see the information in several places at the same time, how do I subdue that analytically so that I still come to the correct kinds of conclusions without confusing myself and my customer?

I think that intelligence really will be engaged in sort of a battle of wits with the best and brightest on the planet. If I were studying it, if I had a long career ahead of me in it, I'd be pretty excited, because I can't think of a more interesting time to be in this business and to be characterizing it for the future.

Now I want to finish my prepared remarks with an example I use on occasion: the characterization of a crime versus an attack. This is a pretty young group, so I've got to work this out a little bit in my mind. I hope that you'll fight back when I use it, but I want to use it on you anyway.

Let's suppose I've presented to you a set of complexities that would at least make you interested in thinking about a rich set of solutions with regard to the shared interests of national security, law enforcement, and industry. Let's also assume that you became a little bit interested in the fact that it now has global proportions; that this unique sense of strategic sanctuary may link us, rather than delink us; and that there's important business in there for intelligence officials to perform that would change the way we do analysis. We'd have to think much more agilely about transnational threats and so on, and we would subdue these concepts of simultaneity and all that. Then you would finish and you would say, "But, Ken, it's not a problem." Where you should have taken me was, "All this is criminal activity anyway. There is no evidence in any of these characterizations we've used that any of this is in effect. It's all seen as domestic, and it's all seen as a crime."

In the industrial age, one of the things we've been very proud of is that we've always protected our strategic sanctuary from attack. So I turn the TV on, and I see the World Trade Center on fire. I see smoke coming out of the Twin Towers. I see people coming down the stairs. I see the cops and the firemen and all that. I'm from Texas, so I'm kind of going, "Hey, it's New York; not a big deal. We're not worried."

Suppose I say, "Well, wait a minute, let's have a discussion. You're wearing a uniform and you're serving the nation; it's your responsibility to defend it. That's the global nerve center for the marketplace of the United States. There are a dozen city, state, and federal branches in there. There are several nation state relationship offices. The telephone switch for the East Coast is in there. The telecommunications switch for Wall Street is there; all Wall Street transactions go through the World Trade Center, and approximately $1 billion a day is traded. If you're an industrial age person, that's a strategic target, and it was attacked."

We Americans watched it on TV and we said, "No big deal. The cops have a problem today." We did not get the wake-up call that our strategic sanctuary is threatened; is vulnerable, in this case, to a transnational threat. We didn't have a vibrant discussion about the difference between a crime and an attack that was relevant to the nation's strategic interest. There was a clear understanding of what the shared responsibilities were, and in that clear understanding, the wake-up call was largely unanswered in the American context.

So it's interesting to try to work that out in your minds. I gave you my Saturday scenario. If we were attacked virtually, and you saw it as criminal activity, then I would say, "Call the cops." If you were attacked virtually, and you saw it as a legitimate national security penetration of your strategic sanctuary, whom do you call? There is no definition of that as an attack, and there's no designated element to respond to it, strategically or tactically. Even if there were, they don't have anything but tanks, guns, and ships to do that.

It's fairly disquieting if you shift some of this over into attack as opposed to crime. So one of the long-term resolutions that I think has to occur in sorting this out is: How do the allied nations of the world who have shared interests start to deal with attacks, as distinct from criminal activity?

Okay. I'm finished.

Student: Sir, in your comments about changing the role of intelligence, how do you perceive the mix of the type of information intelligence looks at? Does it spend more time on open sources, looking at other than covert collection and technical collection?

Minihan: I want to give you two thoughts on it. You clearly touched on one. We will have access to much more information, and it won't necessarily all require what I might describe as the most delicate of investments in operations to get it. So, to be technical about it, one part is that access doesn't equal collection. Put differently, we want to go where the information is, not do what we do now, which is suck up the information and bring it back. I think that will become less expensive but more complex.

The second one is equally interesting. If you want to analyze infrastructures, then you don't just want to take pictures. You want a display of the battlespace; you don't just want to see a picture of it. You want to understand how it works culturally, how it's set up in terms of its infrastructure, and what the relationships are between the telephony, the power, and the military command and control. That template requires you to have a very different drilling process than we do now, because we only go to the topology part now, and you want to see the battlespace underneath it. So I think it'll be both much broader and much deeper with regard to what you want you want to do, which is get the detail.

Student: Do you have resources for that type of job? Do you think that NSA is sized for doing that imaging?

Minihan: Let me answer it differently, in terms of the intelligence community. If you ask, "Can the intelligence community do that job?" my answer would be yes. But the intelligence community is driven by what's known as the intelligence requirements process, and that process is, by and large, char-

acterized as industrial. "I want pictures of buildings. I want ...." So it's a requirement set that is not relevant to the requirements you want satisfied. What you'd have to do is completely republish the collection requirements, and think about the relationships between HUMINT, SIGINT, and IMINT and how different those are. They are a set of enablers; in other words, they aren't stovepipes anymore, or distinct product lines of their own in their own context. We're producing a display; we're not giving you pictures of buildings. So, yes, we can get information that is much broader and much deeper, but the only way we can afford to do it is if we completely revise the requirements process.

Oettinger: I hear you say a couple of different things. Let me see if I understood them. It seems somewhat contradictory, because if I heard you correctly you said, "This is all technology driven." Yes, technology has created infrastructures that have this transnational character, et cetera, but technology, in the sense you've talked about it just now, also has the means to coming to grips with that. Each time I hear you expressing concern, it's less over that than it is over the fact that you have postindustrial technologies and infrastructures, but industrial age mindsets and industrial age mission statements that don't seem to be congruent with what the new missions are. Am I misreading you?

Minihan: I don't think so. I sleep at night because I think I do my job. So, I am not one who says, "The world is folly." I am one who says that we're in a significant state of change, that there is a leadership issue associated with that state of change, and that we have to make some very important decisions.

I think we can do those sorts of things. If you promise you won't share this with my Joint Requirements Oversight Council, this issue is much easier for me to speak to younger people about than it would be if I were sitting in the room full of senior Chamber of Commerce leaders. So in terms of the generation that you are all learning and gaining from, things will be fine. That's why I framed the question not as, "Can NSA do this by itself?" but "Could the American intelligence community do it?" I think the answer is yes, but it has to change its requirements set.

Student: Going back to your example of the World Trade Center, when there is a physical attack, the question whether it's criminal or an attack, as you mentioned already, will determine which agency should be called, whether it's the police or the NSA. But when we talk about cyber attack, to call it an attack means that the NSA should respond. Maybe you should put more responsibility for national security on civilian agencies. It means a broader definition of national security.

Minihan: I think you're exactly right. I would actually have it both ways. I would make it broader in both. You went in two directions. I'd agree with you, and make both broader.

There are shared responsibilities now, relative to the World Trade Center—a physical attack, in that context, that happened in the United States. One ought to have a rich set of options: not just law enforcement and not just national security. You ought to have that same set of rich options on the virtual side, and they wouldn't all be national security.

Quite frankly, one of the arguments I'm trying to make here is that the major investment is institutionally made out of our industrial base. It always has been. It will be essential for the commercial side to make most of the investment. It's not something that the government can go off and pay for on its own, so that all the citizens can go to sleep at night and say, "Okay, we have a cyber army, so we're safe tonight." You make a correct point.

Oettinger: But one of the difficulties of the private sector doing it is that the private sector is perfectly willing to take a hit if it's part of the normal cost of doing business. Stores every day get robbed blind on pilferage and one thing or another. That's the cost of doing business, because otherwise you get so secure the customer doesn't want to do business with you. Nobody wants to go to the department store or supermarket and get frisked at the entrance so the store can avoid

whatever the current normal rate of pilferage is—between 5 and 10 percent. On the other hand, if the pilferage were part of a Libyan effort to do something or other, there'd be a different attitude. What does the private sector do, or how do you allocate the responsibility jointly between the private sector and the government to sort these things out, so that the department store can tell normal citizen pilferage from a concerted attack to demolish the banks or the supermarkets or whatever?

Minihan: I definitely would agree there's a certain local operating level that one would tolerate: shoplifting at 3 percent or whatever. At the same time, when we opened ATM machines up and people were being shot using them, that was no longer normal. Somebody said, "I don't feel like getting shot just because I'm the only one in 10,000 using an ATM." So we responded to that. That, in my view, is a distinction. If you take the cellular phone industry, as its loss rate goes up, at some point the customer is going to say, "I don't want to pay that fee anymore. I want a more secure system."

If you move that to the other end, to the Libyan example that you used, then in my mind that migrated the discussion over to national security. Let's play out the Libyan scenario just for the heck of it. We're here Saturday morning, we've had a virtual attack on Wall Street. We don't have a smoking gun, but we know the Libyans practice information warfare. We know they have an excellent capability to do intelligence. We know that they have trained some people. We understand that we won't be able to prove directly that they did it, but it's pretty clear that they're in the top two or three who are responsible.

Since it was Wall Street, this just cost you about $4 billion. The stock market has fallen by half. The President's kind of in a bind here to respond. Libya doesn't have a stock market, doesn't have big telecommunications, and doesn't have huge investments. They're not too vulnerable to a virtual counterattack. "What do we do, coach?" Minihan says, "Let's go bomb them!" If their vulnerability is in their physical domain, then we need to establish in their minds that we will respond in that sense.

Policy makers are now faced with some pretty tense situations. You don't have a smoking gun. The delicacy of operating in the network is lost. You do have an option, but that option is relatively violent, and it's going to show up on TV and so on. But if you don't exercise it, you have no deterrent, because they will not present you with the same vulnerability that you present to them. So, you have to exercise some deterrent response.

Oettinger: But I think that what I hear there is a false distinction between the physical and the virtual, and it helps set up a false dilemma here. When somebody sticks the tip of an umbrella into a guy on a street in London or in Amman, that's a small amount of energy, but it's regarded as pretty nasty and physical. Now, if you reduce the energy by an order of magnitude and change bits in New York, it's still physical, and it's just as much of a violation of physical space. I don't see why you are calling it virtual. It is nonviolent.

Minihan: I disagree, but let's assume we leave it there. I'm still making the point that Libya is not equally vulnerable, so I want to bomb them. You just said it's okay, because you said there's no distinction, so I'm out of here.

Student: That's horizontal escalation.

Student: It's part of deterrence theory, and I think most people at the international level would argue, "There's no smoking gun, so whom are you going to bomb?"

Minihan: I want to bomb Libya. I'm saying that I know they're in the top two or three, and I'm holding them accountable.

Student: Bomb all three then! Why did you pick one? That's where it began to get to me. You need the security services to be able to identify the target to use your asymmetry against.

Minihan: I'm living with our disagreement, but since you said there's no difference, I

want to go bomb them. "I want your permission, sir, and I want to do it now. I don't want any time to pass here. We just had our attack. I want to get right back in their face, so you need to hurry up and get this decision made."

Student: But then how about Iraq, *with* a smoking gun?

Minihan: Why is he so sure?

Student: I'd like to mention a situation that happened a couple of years ago. A foreign source sent chain e-mail that was received by a lot of people in the Department of Defense. It was all about some little girl who was in such terrible trouble, sick, whatever. For some reason, when it finally got out to the middle of the playing fields in southern Illinois, it pulled everybody's heart strings, so they all sent copies to their 10 closest friends. Within 20 minutes it completely shut down the base infrastructure at U.S. Transportation Command, and only because of a smart sergeant was TRANSCOM not completely taken off the air and separated from all the aircraft and the ships and the railcars they're tracking around the world.

Was that an attack? Were the American people who passed that along guilty of criminal stupidity in helping it? There's a place where it really gets blurred between criminality and attack. When the originators sent that e-mail, did they have the intention of doing that?

Minihan: You're not only correct there. You might argue it was orchestrated, and I'll take the point, but let's assume it wasn't. Let's assume it was as you just described it.

The other part that is interesting is that right now most of the reporting we get begins with a sense that the system wasn't working. The way we usually think now about those kinds of things is, "There's got to be a problem in here. This could not have been orchestrated." We don't go to, "Let's look for evidence that suggests this was purposeful." So what we find in most of our exercises in real-world reporting is that it takes a long time for the victim to move away from, "You know, this damn stuff's just not working. I don't understand why I can't do ... (whatever)," and finally get over to, "I wonder if there is a reason why it's not performing as I expected. Why isn't the service the same service we were accustomed to?" So it's taking our institutions a long time to develop those information highway standards of conduct so that you can make the distinction.

Look at the financial industry as an example of the way that you try to set up your international relations now. If there's no difference here between bits and money, I just stole a million bits, and it turns out that when I push a button it becomes a million bucks. Right? I just did that. So you just lost that million.

If that phenomenon is occurring, how does the bank report it? We accept that a robber can go in and rob the bank, and we just went through a discussion that said everybody understands that occurs every now and then, and people don't all withdraw their money from the bank. But the banking industry, right now, is worried that if it begins to report electronic fraud and criminal activity, the trusting relationship I have with bank X will cease and I'll move my money somewhere else. So they don't have a way to report in the context that they can report a physical bank robbery: in a way that protects their institutional ability to do business. Therefore, you have both the phenomena of not recognizing it in the larger population and of the inability to report it when you can recognize it because commercially it's seen as representing a larger vulnerability that might cause me to move my business.

One of the things you need is a set of federal, state, and local reporting criteria. It's just like in aviation: if there's a near miss you can report it, and people don't fault the airport and put everybody under arrest. They go investigate and find out what they can do. But it is okay to report a near miss. It is now not okay to make the kinds of reports we need. Remember the discussion we were having at the very beginning about what kind of activity is really going on. I said it's in that lower part of the iceberg and for any number of reasons we don't understand it yet. One of the things we really do need is an international set of reporting criteria.

Oettinger: It seems to me that the physical versus the virtual thing just obfuscates what is fundamentally a policy problem. Let me try to hammer on that point so that it gets you either to show me why I'm being dumb here or why it's reasonable.

Take the explosives identification business. There's this big argument over making explosives traceable, and the explosives industry would really rather not. But as a practical matter, you could be very sharp about pinpointing explosives and where they are manufactured, and have a signature, and make the whole thing traceable. You could do that with banking transactions, so that for any packet or whatever that arrives, they know it's from me or from you or from some third party. They don't let it through the firewall, and they ask a lot more questions.

Now, that would shift the presumption to one that would get every civil libertarian in the country up in arms, but you could pretty much guarantee 100 percent safety of all your assets. Then you can shift to the argument about how much safety you are willing to relax on in exchange for greater civil liberty. But that's fundamentally a policy question, not a question of technology, and not a virtual versus physical kind of thing. It just seems to me that all your illustrations go back to questions of policy and politics, not to physical versus not physical.

Minihan: My sense would be that it's more than just policy. The government portions could be solved by policy. I don't think the commercial citizenry parts could.

To go back to an earlier part of the discussion, I'm agreeing with you when you suppose that if we had security services in the network, we could deal with inappropriate conduct today as we can deal with inappropriate physical kinds of activities. And then I'm telling you that we don't have those services.

Oettinger: Understood. But what's in the wind then is a policy debate.

Minihan: I just think it's more than policy.

Oettinger: What is more? I guess that's what I'm missing.

Minihan: The general consensus. I can't say--in a policy that starting tomorrow every information technology investment will have a security service apparatus in it.

Student: Sir, the U.S. government could. The Congress could pass a law. It's not going to happen.

Minihan: I'll grant you the law, but we cannot make a policy that would cause that to occur. And if we did, I couldn't tell the British they have to conform to it.

Student: That's the challenge.

Minihan: Even if we got that part done, I could not go down to the local level in Louisiana and tell them they have to conform to it. So there's more to it than a policy.

The other thought I'm sharing with you is that given that context, our ability to use the technologies that we're discussing is contingent on our developing something that precludes, generally speaking, what I would describe as acceptable misconduct. Unacceptable misconduct will then fall to either law enforcement or national security, because there will be nation states or terrorists who do that, and they will be outside of the system. They'll say, "I don't care about your policy and your laws, I'm doing whatever." Those will then fall into the legitimate domain of a major law enforcement effort or a major national security effort. I don't think you get it all swept up under whatever we could reasonably afford given our national solution, which has international implications.

Student: Professor Oettinger and I have talked quite a bit about this. One thing I think we do, though, is enter into this discussion of technology and policy and their relative priorities by making so many assumptions about what policies are just never going to be passed. Politically, it was an evaluation that more government regulation in this realm is just not salable in the 1990s, and therefore, we don't even consider some of the policy-based solutions or incentives we could provide before we start to consider the benefits of those solutions. We were just whispering about standards and creating standards where

we could. If there were standards built in for a lot of security and they were mandated (even though that's not something that people would like to hear these days), it would draw a lot of technological followership into creating these kinds of keels that are necessary in the 21st century.

Minihan: I agree with you. Let's play the policy thing. Suppose the SECDEF said that as a matter of policy, by January 1999, all operating systems that the Defense Department has, and uses commercial products for, will have the five elements of the security services we discussed. We're to buy that from all of you in industry, and use it. I'm going to work with my allies so that within NATO, or any other environment, I can have an architecture that allows me to have those same services across international lines. You can do that. Now you've created a customer base for the environment that you've talked about and it's well within your policy domain to do it. It doesn't change the other two major components a bit, but it has a huge impact on getting it started.

If you read Dr. Hamre's one-page summary in this longer document[3] ...

Student: Here it says that if you do that by January 1999 and then you want to be a contractor for a major weapon system by January 2000, you're only going to operate in a paper-free environment, which means using a computer. This means that the commercial contractor (this is not the military side) has to have those information systems there. The DOD policy does give some actual policy incentives to the commercial world, not just wishful thinking ones.

Minihan: I'm agreeing with you. What I'm saying is that we then set a standard. We could say, "These are the standards we want to have in our operating systems," and, for the most part, just let industry build the products to those standards. You're correct: -- they'll then become the de facto standard. Where you used that argument, I prefer to use the term "specifications," but "standards" is okay with me.

Then you have the dialogue just as you did. There's clearly a customer base for you. There will clearly be something that institutions that are worried, such as banking and telecommunications, will pick up on and use. As all of you who are in uniform already know, over 95 percent of the business we do in Defense is already in the commercial infrastructure, so it's going to be in all of that, too. It doesn't deal with the other two regimes, but I think it's an excellent start.

If you look at this whole 100-page document, there's a one-page, sound-bite kind of thing that finishes with "by January 1999, the Defense Department has the intention ...." I wrote that sentence. That's the intention of that sentence being there, to make us a customer for those services. The trick now is to figure out what we mean by the sentence.

Student: I'd like to take a different tack here, referring back to one of the last points in your prepared statement about how we respond to attacks of a less obvious physical nature. Some propose yet another branch of the armed services, namely, an information corps. Just as the Army is supposed to have dominance on land, the Navy in the sea, the Air Force in air, there would be sort of another one in cyberspace. Do you see that as feasible, something that would help? How do you see that playing out?

Minihan: That's interesting. It's a good question. In our dialogue, you've heard a couple of times that I'm kind of saying, "I'm not sure you can get there off the platform we're on now," and Tony is saying, "I'm not sure you're right, Ken. Tell me again."

Our CINCs are arranged geographically, and I've just kind of said, "That ain't the right way, because something bad can happen to that CINC, and it's not his area of responsibility." That's not the way to do it. So we either have to attend to the way we think about our responsibilities, or we need to put someone in who sees across them. It seems to me that those are your two options. That's

---

[3] John J. Hamre, *Defense Reform Initiative—The Business Strategy for Defense in the 21st Century.* Washington, DC: Office of the Secretary of Defense, November, 1997. The document is also on the Internet at http://www.defenselink.mil/. Dr. Hamre is deputy secretary of defense.

a rich debate in the department right now. You hear both advocacies. I'm less into the cybernaut. What I played out to you is that we have to change the way we do intelligence business, and we have to change the way we do operational business. That, I think, is more characteristic, and that's a better solution than having a special unit, because it turns out that this matters in air operations, it matters in ground operations, and it fits nicely into your kit bag, as opposed to having a whole separate bag you've got to carry.

What does that mean for intelligence, for example? What it says is that for these guys who are here studying intelligence today, and going back to the military, intelligence in 2001 will be a combination of the computer career field, the communications career field, the operational career field, and the intelligence career field. That's the career field they'll be in—a team—as opposed to a distinct intelligence career, which is the way the CINCs are now set up and the way they fight. You're not just in intelligence anymore. That would be my preference, rather than creating this distinct corps. But both are lively in their discussions. Generally speaking, the space component is the one that argues the best for the corps, because it is a component that sees virtually anyway, if you can use that phrase. The others worry when they hear that discussion, because they see a geographical loss if that were to occur.

Student: Could I just ask a follow-on about capacity, or resources allocated to this? When you talk about the fragility of strategic sanctuary, it sounds as though there's a growing number—if not growing volume or intensity—of different threats we can face in addition to the previous ones, while at the same time, as we see most clearly illustrated here, there's a contraction of resources available. Within an even smaller circle of resources available to Defense, do you see that these new threats can carve out a reasonably viable chunk of those resources available?

Minihan: I think they have to. To get back to the discussion we had about industry, how does the government turn to industry and say, "I want you to spend money on security services," but at the same time say, "You guys in Defense keep buying jets, boats, and tanks." It has to happen. You pick it: it's one less F-16 wing or it's one carrier battle group less. I don't know what it will be, but my view would be that eventually it will come out of those funds.

People in our business who would counsel our leadership in terms of being taxpayers would say, "There is a point where we just prolong the fight, but we still lose." You've got to find where you stand relative to that investment, and the investment has two components. It can be sized differently, but there also is a point where if you can't reasonably deter, you end up fighting a lot more, so you've got to find where that calculation comes out. But Defense has to invest. Nobody's going to look at $200+ billion and have Defense say, "We don't have enough money." When I'm joking with my fighter pilot pals, I'll talk with them like this and they'll all say, "Ken, this is crazy. You don't get it," and off we go.

My point is that you finish the discussion by saying, "Well, what if I'm kind of right here, and what if the nation feels vulnerable? What if it wakes up someday and it has what it thinks of as an electronic Pearl Harbor?" It doesn't have to be like an industrial Pearl Harbor; it could be just a shaking of their confidence in the developing network environment, in the context that they see it being as important as electricity: "This is important to me, and I want to be able to use it."

They turn to the government, and the government turns to Defense and says, "What do you think about this?" Defense says, "Well, I don't have enough money to invest in it. My thinking is not clear on whether it's geographical or vertical, and I'm not certain whether we need a corps to work on it, but I've got this two-MRC (major regional conflicts) theory. Could I tell you about that?" You're not going to be relevant to the nation's strategic concerns. I think a very important move is to make Defense relevant to that, and you have to pay for it. NSA has paid to invest in this out of its own declining budget because it's the right thing to do for the nation. The wrong answer is, "Hey, I'm downsizing. I'm sorry. I can't get over to you. Let me know when you go down the third time and I might."

It will be a very tense discussion, because we're already not buying anything new. Now you're talking about shifting dollars, which, essentially, are investments in states and cities for things that are ongoing. You're not talking about shifting money that has not been invested yet. So, any decision would be seen as kind of like closing a base. There are some big political interests to be worked out. But I think Defense has to invest.

Student: You mentioned how we're organized geographically in the CINCdoms, and that's true for a majority, but a significant, nontrivial portion of the Defense Department's organized CINCs are not geographic, such as TRANSCOM, Space Command, and Strategic Command. One of them, Strategic Command, is nominally a warfighting CINC. Renaming or relabeling any one of those or creating a whole other CINCdom that says, "We're Space and Electronic Warfare," where it subsumes the Intelligence Command, or whether you say it's TRANSCOM, a support organization, not a warfighting CINC, or whether you say it's STRATCOM, the cyberwarfighting CINC model, you still get a structure that the military should be comfortable with. It's not something brand new or unique, where we don't necessarily know how to do cyberwar, but we understand the command structures they're being involved in.

Minihan: That's why I said the option for spinning off from a geographic CINC is Space Command. It's normally the one you'll hear as a logical functional CINC. The reason there's some comfort with Space Command is because it has this kind of world-wide view. The reason for discomfort with Space Command is that it's disconnected from a physical basis. I hear 51:49 discussions all the time, when they go on. My view is, it will be resolved about as slowly as the political landscape we've just discussed. I don't think you'll see any dramatic movement. It'll be evolutionary, and it's going to take a while. The reason I say it's going to take a while is that if I go into your office and look around at what you've got there, I can tell a lot about how far we're going to get with this discussion.

Oettinger: It's quite understandable. The prevailing, ruling powers, if you will, in the military are the tank drivers, and the plane drivers, and the ship drivers, and they're not going to give him money for doing new things with electronics stuff. It reminds me this is not the military alone. It's now many years since Nate Pusey was president of this university and I was running some of the university's computing facilities. I went to see Pusey to ask him for money for something, and he leaned back in his chair and he said, "Professor Oettinger ..." (and I knew from the tone that he wasn't about to do it) ... "Harvard did not get to be where it is by spending old money on new things." My guess is that that's sort of true in any institution. You don't get to where you are by having spent tank money on electronic gadgets.

Minihan: You've noticed in our discussion this afternoon that it depends on how you characterize what I've told you. Typically, I'm seen as a sort of cyber geek. We've always gone over to the "Wait a minute; what's so different?" I never said that. If you noticed, I said it's lethal/nonlethal. I recognize the asymmetry. I think we ought to use both. But you bring the lethal physical part into tension by offering this other component.

Now, my argument is the one that I shared with you. I feel good about it. In other words, I think it's an opportunity, and we need to invest in it relative to all of the arrows we want in our quiver, not only what you might describe as our physical arrow. If we weren't going through this great era of downsizing, you might find greater receptivity. But for the most part, leadership's ability to invest right now is really diminished.

Oettinger: But by casting it as lethal/nonlethal, you're helping the other side make their case. It's not all that nonlethal, and lethality is still necessary because if there weren't the muscle to back it up, then all of this cyber stuff would be laughed at. You need the implied threat that if you don't accede to the cyber something or other, I'll blow your brains out.

Student: It's just like that movie scene, "I know karate," "Oh yeah? If you do, you're dead."

Student: I know, "Cyberwars."

Student: Sir, moving away from cyberwar and other threats, how is intelligence responding to the counterproliferation effort? Assuming we have these new threats, since the Cold War is over, in addition to cyberwar we also have the proliferation of nuclear weapons.

Minihan: You ask an excellent question. Intelligence really has four main areas: military support, policy support, transnational counterproliferation and those kinds of things, and then counterintelligence. The growth is in the one you mentioned. So we're clearly worrying about the transnational migration of nuclear weapons, and how we think that will work out. The worry is in two areas. One is not so much that it results in what you and I might think of as a Clausewitzian weapon system: it's a rocket, it's going to launch from a command and control environment, it will have to be controlled, it will be targeted, what if it's floated in or brought in, or what if it's not? That's one big part.

The other part is that if you take countries like Russia, it's like a backyard sale. In other words, they're available, and there are, obviously, nations that will buy them. So, it's a hugely important issue. As you would expect, you have to grow to understand it, because if it's not Clausewitzian, now you've got to understand how they move things like that around when they don't have formations and people in uniform and things like that. So it's a completely different world we've built.

What you're seeing most of us do is reorganize and develop a different analytical cadre based on infrastructure analysis, as opposed to air order of battle, ground order of battle, and all that sort of thing. We're doing a lot better against it, and you see that played out in the newspapers and so on as you see demarches and what have you against the sales.

Having said that, you're never going to be 100 percent successful at keeping terrorists from acquiring those weapons, so the scenarios you've got to play out in your mind are kind of the Khobar Towers plot, but extended to take nuclear weapons into account. I think we will ultimately need the ability actually to deal with that situation. If the terrorists have succeeded, we'll find out, but now what do we do, coach? Do it a lot better! It's a completely different organizational and analytical collection of problems.

It turns out that, just like others, we have smart people and if we put smart people in to do tough things they'll do okay. But then the response part is equally difficult, because now there's no accountability. We're back into the non-nation state part of the business. So, it's one of the four complexities. I think we will be fine, but the terrorists will have successes, and we're going to have to find a way to deal with that relative to our own continental United States.

To get back to the discussion we were having about Khobar Towers and all that stuff, normally you don't give the U.S. military a domestic role. But this is one that's clearly going to call for it. How does the military deal domestically with that, as opposed to every local police guy being able to take care of one of those weapons? So, I think you'll see a growth in the mission area.

Student: In the beginning, you referred to a change of the intelligence activity in the 21st century, and you said that intelligence will not only support, but also participate in actual operations. The more you participate in the actual process, the more you expose yourself to the risk of politicizing the intelligence community. How would you strike a balance between the need for further participation and the increasing risk of politicization?

Minihan: You ask an excellent question. That used to be the nature of the class that was taught here. Senior intelligence officers used to come here; I don't know if they still do. I came for a two- or three-week course, and that was the key component of the course. Do you simply give information and disregard how it's used, or are you responsible for its being used? If they ask you your opinion, do you supply your opinion? We are leaving the era where the answer was that we avoid politicizing the process by not partici-

pating. We're entering the era where we're not going to politicize the process, but we recognize participation.

To deal with your politicization issue, your worst nightmare, really—and it happens a lot—is when policy makers want to make decisions that are inappropriate relative to the information, and you have to say, "That's not what the information supports. That's not there." They want to hear that there's an accountability underneath there, and if it's not there, you've got to tell them it's not. So it's become almost as important to tell them what we don't know as to tell them what we do know.

General Powell has a great saying. I worked for him for a while. He'd call you in and he would say "Here's what I want from you." He's very clear; he's a very smart man. Then he would say the following: "Tell me what you know. Tell me what you don't know. Tell me what you think. And make sure I know the difference."

Student: You touched upon something that's kind of key here, and that is the transnational organizations, and how the threats made abroad now could be continental. We've got agencies like the FBI that really are chartered for domestic issues, and CIA, which is chartered for international issues. We have the DIA and other intelligence sources also. How do they work together, given their different constraints by charter, to shape the environment as you see it in the future?

Minihan: Let me play that back a little differently. The fastest growing mission area overseas is with the FBI. So, law enforcement is not defined geographically anymore, and that's okay. That's consistent with what I've said to you this afternoon. The FBI's overseas responsibilities, as you saw, for example, with Khobar Towers, have grown substantially, and they're actually one of the few organizations that has a fairly massive hiring program because of its growth. So, I see the charters as being less the issue than what the new technologies have given us the opportunity to do, and how we use the charters that we have to take advantage of the new technologies.

Remember I told you that HUMINT, SIGINT, and IMINT are enabling. The CIA and the FBI now have an enabling relationship overseas, which didn't used to exist. You want to distinguish clearly when you're doing the HUMINT collection covertly or overtly under CIA's overseas charter, and when you're performing your law enforcement overseas. You want to make those two enabling as opposed to a distinct law enforcement and a distinct clandestine HUMINT operation.

You have the same thing technically. If you think about infrastructure analysis and a changed set of collection requirements, then CIA and NSA have a very close relationship overseas, which is an enabling relationship. I think it's less a relationship constrained by the charters than a completely different set of relationships within the charters. So when I go to CIA, for example, I talk to them about their responsibilities to enable the SIGINT environment, which is completely different than when we used to talk about it only as a HUMINT environment. When I do that, it depends on what generation you're talking to. The seniors say, "Call me if you need help," and the young people say, "That's right; we need to work in this area." So you have the natural generational issues in there.

But I think that what you'll find is not as much change in the charters as a recognition of the new technologies and how they ought to work. That will eventually, in the long term, result in a reorganization of the intelligence community, but in the near term it will be characterized by a completely different set of cooperative relationships.

Student: Do you see a change in the way we handle intelligence organizationally? Could we see the FBI and the CIA maintaining their structures as they are today?

Minihan: For the near term, yes. The FBI is an important component of the community, but I don't classify it as an intelligence agency as I do CIA and NSA and NIMA (National Imagery and Mapping Agency) and so on. So, to distinguish between the FBI and the intelligence community, I think that in general the FBI, while it will change its operating parameters within its charter overseas

and so on, will stay as a coherent whole overseas. It will have a completely different relationship at the federal, state, and local levels, because when we get done with the domestic encryption and so on, they'll be operating in a completely different environment than they do now.

With regard to the other elements, I think that the enabling relationship I just mentioned to you will first manifest itself as a different era of cooperation and some changed operating parameters, which will eventually result in a reorganization of the community. That's the correct answer. The incorrect way is the typical American approach, which is: there's change coming, let's reorganize. So we divert everybody's attention and time to changing their sweatshirts, and where they work, and their telephone numbers, and all that, rather than letting them subdue the new operating conditions and then, to use a gross analogy, once we've got the buildings all built, putting the sidewalks in when we see where they walk. Once we get that all done and we see where they walk, then we'll put the organizations in around that new construction. But it's okay to let us go through the change of our operational conditions and then organize around those, rather than what you've seen in the past three or four years in the form of any number of studies on what some organization or function will look like.

Oettinger: You've just made a persuasive argument for the need of something approximating an electronic Pearl Harbor to change the structure of the military. One of the reasons for the situation with regard to the FBI and the CIA overseas, as you've just described it, is that there have been enough incidents to warrant those kinds of moves toward cooperating, which would have been unthinkable before. They responded to real situations, but they haven't merged the two agencies, because law enforcement functionally remains different from pure intelligence gathering. Their aims are quite different.

It would seem to me that there is the potential for similar gradual adjustments within the military. I don't think one needs to wait for a Pearl Harbor. There may be intermediate things. The military does operate domestically. The Army Corps of Engineers has met a set of peacetime, domestic needs now for a century. That domestic collection of intelligence got the Army into trouble 30 years ago is another story. But it would seem to me that there is no reason why the military can't adapt in precisely the way you just outlined, as situations warrant. We've been lucky not to have any of those.

Minihan: You're right. An excellent experience for several of the CINCs was that we had our first information warfare exercise. The CINCs got some exposure to their vulnerabilities, and they responded to that. They're not dumb; they're responsive, and they want to do the right things. So, you're right that some situations will lead the military to adapt.

But to get back to the discussion we were having at the other end of the table, I think that without an investment, you're still playing on the margins of what substantially is going to be a big change. Now the question is whether the wake-up call precedes or follows. The reason that there's a NASA is that the Russians put Sputnik into space and Americans felt their strategic sanctuary was threatened. They built an agency and said, "I'll meet you on the Moon." So I'm just saying that if that wake-up call comes and the Defense Department doesn't appear relevant to the wake-up call, they're going to go somewhere else.

Oettinger: But you're now reinforcing the other point you just made a moment ago. The creation of NASA was cosmetic bullshit opposed to Sputnik. There were space programs in place. Eisenhower had put them into place quietly.

Student: NASA existed before. It was NASA, but it wasn't called that.

Oettinger: It had another name: NACA (National Advisory Commission on Aeronautics). There was a space program. It just was at a low level.

Student: We just decided to upgrade it to something meaningful, but we didn't do it until after Sputnik.

Minihan: But the upgrade didn't occur inside the institution of Defense, because there wasn't confidence that they had it right. So they upgraded somewhere else. All I'm saying is that if you decide to upgrade things, and we don't appear relevant in Defense, then they could take that business somewhere else. If that were to occur, it would come out in a sense. So you've got to worry about the chicken and egg part of this if you're in uniform in Defense.

Oettinger: Yes, but from a national point of view, whether it was NACA or NASA didn't matter.

Minihan: To pursue your argument, you're correct when you say there are a lot of policy things the government could do under the Defense Department hat that would be leadership oriented and would be useful. I think the nation would expect Defense to make some useful policy decisions.

Student: You might want to consider using something like what we were talking about earlier—an electronic Louisiana Maneuvers instead of an electronic Pearl Harbor. There's probably better resonance, in that "Louisiana Maneuvers" was a military maneuvers spec by the Army prior to World War II that sort of prodded them in a different direction.

Student: I recently spent some time looking at exercises the Air Corps ran between World War I and World War II, in the early 1930s, about how bombers were going to get through. We built two kinds of B-17s (they would have merged in the late 1930s), and they were faster than the fighters. We got into a period by the mid-1930s where the bomber could always get through, because we learned technological lessons from some exercises in the early 1930s that we then had a hard time unlearning when radar and defensive fighters came about in the late 1930s.

I'm not sure cyberspace fits this model exactly, but right now, it's generally believed that hackers can get through pretty easily. There's an emphasis on dealing with offensive dominance. We need to stay aware that the technology changes and that some defensive means, like radar or faster fighters, might come about. We can learn the wrong lessons from exercises unless we keep exercising and keep learning.

Minihan: In any reasonable scenario you defend first, so the first priority should be an information assurance strategy. You're correct in that sense. That's why I said that if you see it as conflict in the information age, not as information warfare, you move away from the flashiness of the offense and you look at it in a much broader sense. You're right. That's the other thing that's in this announcement here:[4] a national information assurance strategy.

Student: In information assurance strategy, if a significant part of our national power actually resides in the commercial area, what does the intelligence community have to do in counterintelligence to ensure a commercial advantage?

Minihan: It's a hugely changed relationship, in my view, which you've got to think your way through. I think we have to share threat information. I think we have to share information on vulnerability, in the sense of our understanding of what really is possible. We had this discussion earlier: you always get over to, "Well, tell me what to do." Industry does not have a good sense of that.

Lastly, if you think of counterintelligence in the context I think you mean it, then industry has no sense of what it looks like outside their own industrial base. If I go out and speak to the telecommunications people, they don't think about the bankers, or the railroads, or the electric grid and so on and so forth. You find each one of them focused on, "I need to make the ATMs secure; I need ...." "So what about the power?" "That's not my problem." Well, it clearly is. So you have that complexity to add from the CIA perspective.

Now, let's play the last part out just so you drop the other shoe. Everyone knows that the intelligence community does not work in the domestic environment. Right? So now what is a domestic environment? Where

[4] See note 3.

does AT&T's domestic environment begin? I don't know.

Student: It fits nicely with your discussion of cyberspace.

Minihan: Yes. So you have to figure your way through that because we're back to: there are laws here, we want to obey the laws, and the law has a strong domestic prohibition.

Oettinger: Sir, thank you so much for an enjoyable discussion. Before we let you go, here is a small remembrance of our thanks.

Minihan: This was great. We enjoyed being here. Just getting us out of town was great. I want to return. The way I'm going to get out of this whole thing is that I'd like to give you an NSA coin, which I hope will find its way to your office. It's got the NSA shield on it, and just so you students know, the shield is an eagle. If it were in color, it would be on a black background, which indicates a worldly context. It has a key in its claws for breaking codes. The most important thing is that the eagle is looking to the right, which, in the American context, is looking to the future, which is where NSA is heading. I will leave this coin with you, and any time you need me, just call me.

Oettinger: All right! Thanks again.

INCSEMINARF1997

ISBN-1-879716-54-2