INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

A Conversation with the Assistant Secretary of Defense for C3I
John P. Stenbit

Guest Presentations, Spring 2003
A. Denis Clift, Dale W. Meyerrose, Roberta E. Lenczowski, John P. Stenbit, Patrick M. Hughes, James M. Simon, Jr., Richard Hale

July 2003

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 I-879716-86-0 **I-03-1**

July 2003

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
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)
PDS Consulting
PetaData Holdings, Ltd.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Strategy Assistance Services
TOR LLC
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

A Conversation with the Assistant Secretary of Defense for C3I

John P. Stenbit

March 13, 2003

John P. Stenbit became the assistant secretary of defense for command, control, communications, and intelligence (ASD(C3I)) in August 2001, and now heads the C3I successor organization, Networks and Information Integration. Prior to this appointment, his private and public sector service in the telecommunications and command and control (C2) fields spanned over thirty years. From 1973 to 1975, he served in the Department of Defense (DOD) as principal deputy director of telecommunications and C2 systems; for the next two years, he was staff specialist for worldwide military command and control systems in the Office of the Secretary of Defense (OSD). He has served as chairman of the Science and Technology Advisory Panel to the director of central intelligence (DCI), and was a member of the Science Advisory Group to the directors of naval intelligence and the Defense Communications Agency. He also chaired the Research, Engineering and Development Advisory Committee for the administrator of the Federal Aviation Administration, and has served on the Defense Science Board, the Navy Studies Board, and the National Research Council Manufacturing Board. In 1968 he joined TRW and was responsible for the planning and analysis of advanced satellite surveillance systems; he retired from TRW as an executive vice president in 2001. Previously, he had worked for the Aerospace Corporation on C2 systems for missiles and satellites, and on satellite data compression and pattern recognition. Mr. Stenbit has bachelor's and master's degrees in electrical engineering from the California Institute of Technology, and is a member of the National Academy of Engineering.

Oettinger: We are privileged to have as our guest today John Stenbit. You have had a chance to look at his biography and find out about his distinguished career, so I won't eat into his time by making any further introductions. He has indicated a willingness—indeed, a desire—to be bombarded with questions rather than to give any kind of formal presentation. I know you're not shy, but just to avoid the slightest risk that we won't get off to a start, let me throw the first one out. Could you enlighten us a bit about what pulled your office together—what the motivations were for pulling together command, control, and this, that, and the other thing; what the motivations are currently for creating another office with the intelligence label; and where that all stands practically and rationally? Let's go around. Other questions?

Student: We discussed moving from n^2 communications nodes to n. Could you talk a little bit about the bandwidth associated with that?

Student: I was wondering if you could talk about how the "I" part of your organization is changing as a result of the war on terrorism. What happened to "I" after September 11?

Student: I'm curious about funding. Do you think that you're properly funded? What role does the monetary system play?

Student: Could you maybe discuss the CONOPS [concept of operations] for data management and information sharing? Then I have a second question on the budget. Could you maybe discuss your thoughts on Joint Forces Command [JFCOM] and how the PPBS [planning, programming, and budgeting system] cycle might be reformed to better incorporate joint technologies?

Student: What do you see as the changes in your office as you go from "C3I" to "C3"?

Student: Do you have anything to say about the relationship between the DOD and the new Department of Homeland Defense [DHS], and if your agency is going to be involved with that in any way?

Stenbit: Is this off the record? I have no problem with anyone down here.

Oettinger: Let me spell that out. Anything you say is not for attribution if you don't want it to be; however, we are recording it. You will have a chance to edit it before anything gets published, and we've had no leaks of the tapes in the past.

Student: How is the DOD involved in the Terrorist Threat Integration Center [TTIC]?

Stenbit: I must admit I'm not an expert on that, so I think that's going to be a short answer.

Student: Rob Slade just published a damning indictment of our national strategy to defend cyberspace in *Risks Digest*.[1] The policy is supposed to make cyberspace safe. I wonder if you have anything to do with this national strategy and what you think about it.

Stenbit: I assume the article attacked the policy that came out of the White House about four months ago—and the final version that just came out? Information assurance policy is what you're after here.

Okay, that's a good group of questions. I'll see if I can get through those in forty-five minutes or so. That'll leave enough time for additional questions.

Motivations and what happens when you go back and forth are interesting. Whether it's a "C3" office or an "I" office or a combination of the two, nobody in the OSD wanted either of them to be there, because they symbolize a set of problems that always come up. It would be

---

[1]Rob Slade, "Education and the National Strategy to Secure Cyberspace," *The Risks Digest* **22**, 63, 12 March 2003, [On-line]. URL: http://catless.ncl.ac.uk/Risks/22.63.html#subj1 (Accessed 22 July 2003.)

nicer if it were some sort of clean organization. For instance, when you talk about financing there's a comptroller. When you talk about personnel, there's a personnel office. Because it's the government and the DOD, there is always going to be a policy organization that's looking at what the State Department (or whoever) does from our point of view. Because the DOD spends an enormous amount of money, there's going to be some integration of how we procure and acquire things. Those functions are accepted as parts of the job, and have an evolution of their own. They become stovepipes. They become an entire financial mafia and an acquisition mafia and their attributes all get written into the law.

Both "C3" and "I," in whatever form you'd like to take them, are there because of a different kind of problem. Something went wrong. Something didn't work, and it didn't work often enough and consistently enough that we had to have somebody to task with working on solving that problem. In the period of the 1960s, neither office existed, as I recall. (It was slightly before my time.) In the early 1970s, there was created what was called an ASD(T), an assistant secretary of defense for telecommunications, and there was an ASD(I), an assistant secretary of defense for intelligence. They were parallel to each other, and they were both there for approximately the same reason, which was the demand for intelligence information from the operational side of the military. That meant the information had to be very specific and very fast, as opposed to (and I'm not trying to be pejorative when I say this, but I'm trying to make an allusion that is at least useful for you) sitting and reading things and then thinking about them and writing reports about what you read. The things you have as input are a little bit more privileged as pieces of information than you can get by reading books or newspapers. The intelligence community was really used to large-scale analysis kinds of issues, but the output was in the form of papers and almost books, et cetera.

The interaction of various force components and what was going on in Europe in those days caused people to start to worry and ask, , "Hey, wait a minute! What are the details of the Russian plans for attack? More important, what are the sorts of things that we could measure to get some inferential data that might actually lead to where people would go and attack things at a tactical level as opposed to the strategic level?" I wasn't there, and I can't speak for it, but my sense is that this happened when we first believed that we were actually going to do something other than drop nukes on somebody.

Oettinger: For those of you who are interested in pursuing this topic further, there is a contribution to the seminar by Ruth Davis, who I think was director of defense research and engineering around that time.[2]

Stenbit: She came after this. She was there in the late 1970s, after I left. She was at the DIA [Defense Intelligence Agency] when all that was happening.

Oettinger: Second, we will be hearing in April from Jim Simon, who would represent a somewhat different view of the balance between intelligence in the large versus the tactical.[3]

---

[2]Ruth M. Davis, "Putting C^3I Development in a Strategic and Operational Context," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1988* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-89-1, March 1989), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/davis\davis-i89-1.pdf

Stenbit: He's younger than I am, so his first-hand data probably also come from back in the 1970s.

Anyway, on the telecommunications side I do know what was happening. We were having a whole series of major failures. The North Koreans captured the *USS Pueblo* in January 1963. It took them thirty hours to get the *Pueblo* back to North Korea, but it took us thirty-six hours to find out that there were Marine aircraft on Okinawa that could have intercepted it and saved it. The fact that the Koreans were slow is interesting; the fact that we were slower is even more interesting.

The Israelis called us up one day and said, "If you don't get that ship, the *Liberty*, out of this place we're going to sink it in twenty-four hours."[4] We couldn't tell the ship to move when we got the data back because it was already under the water, because it took more than twenty-four hours for the data to wander in through the system and come out at the other end.

A ton of such cases were going on, and there was a whole committee in Congress carrying out permanent investigations of the failures of Pentagon communications. The DOD telecommunications and intelligence offices were formed at about the same time, and they were both formed because of these problems. Actually, the key for both of them was to get involved in the integration of acquisition, development, policy, and actual strategy. We were able to use computers—the environment was getting more automated—but in those days there weren't any networks. DARPA [Defense Advanced Research Projects Agency] was just thinking about inventing the ARPANET in 1969. I think Mr. Gore got caught up in this a little bit, but what he did was about ten years later. It was basically a 1980 phenomenon—before there was any rigorous and robust network.

On the intelligence side it was the same issue. It was highly compartmentalized. The NSA [National Security Agency] didn't tell anybody what it did; the CIA [Central Intelligence Agency] didn't tell anybody what it did. We were taking pictures in those days, and the people who took them didn't tell anybody what they did, and so forth. The genesis was sort of "Let me have some places to go and work on this problem."

What really happened on the "I" side in 1974, 1975, and 1976 was a whole stretch of congressional activity dealing with the intelligence agencies, undertaken by Senator Frank Church [Dem.–Id.] and Congressman Otis Pike [Dem.–N.Y.]. Some of us were suspicious about what their motives were, but in any case they were certainly effective in challenging a lot of

---

[3]James M. Simon was assistant director of central intelligence for administration. See James M. Simon, "Crucified on a Cross of Goldwater–Nichols," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, July 2001), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/simon\simon-i01-3.pdf , and "Analysis, Analysts, and Their Role in Government and Intelligence," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2003* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-03-1, July 2003), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/simon\simon-i03-1.pdf

[4]For a detailed account, see A. Jay Cristol, "The Liberty Incident," 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_pdf/cristol\cristol-i96-2.pdf and *The 1967 Israeli Attack on the U.S. Navy Spy Ship* (Washington, D.C.: Brassey's Inc., 2002).

issues about the intelligence community. They really went on a crusade to challenge the removal of rights that had allowed the intelligence communities to do certain things, compared with normal systems. You have to remember that that's when Mr. Rumsfeld was the secretary of defense. So when he thinks about intelligence, what he remembers is having to hire ex-Congressman [Robert F.] Ellsworth as another deputy secretary of defense (in those days we had two deputy secretaries of defense, the only time it's been like that), and he had Al Hall as the ASD(I). They spent 100 percent of their time worrying about Church and Pike and what we were going to do and how we were going to do it. It became an enormous drain on the Secretary's time, in addition dealing with all the problems that had caused the ASD(I) to be formed in the first place. We used to refer to that as the "Green Door Syndrome." The guys behind the green door sat there and fondled the data and never told anyone anything about it, et cetera. There was a lot of pressure to try to break down some of those barriers and see if we couldn't use the information more proactively.

On the C3 side, we had started enormously complex programs to make radios interoperate with each other. We wanted to communicate using secure voice. In those days, everything was analog. There were no digital systems, so that meant you had to digitize it. Analog-to-digital converters were rather complex in those days. Then, after you digitized it, you didn't have the bandwidth to send it, so you had to compress it. As soon as you compressed it, everybody sounded like Donald Duck. In fact, if you get a very low-bandwidth digital signal today and you try to compress it, the vocoders are much better because the processing gain is much better, but we didn't have any processing then either.

So the bottom line was that we had to come up with a standard that was DOD-wide, which was 16-kilobit voice, Vinson encryptors, and vocoders, et cetera. Let me assure you, every service already had its own systems, and none of them used Vinson and none of them was 16 kilobits. So there was this first-order problem about how to get the Air Force to talk to the Army, et cetera. Those were very real problems, because the DOD ended up with systems they developed themselves to special-purpose specifications. There were no commercial standards for any of this stuff.

Today interoperability is a lot easier. We may not know whether we want to do GSM [Global System Mobile] or CDMA [code division multiple access], but we can build a phone with both of them in it. We didn't have any of those options then. The phone would have been the size of a refrigerator if we had put both in. We can do TCP/IP [Transmission Control Protocol/Internet Protocol] and anybody can come with any computer and hook it up to the Internet. There were no such systems then. Ma Bell, in those days, would not allow you to buy a handset and hook into the telephone system. It was a "foreign attachment," and it was against the law to attach a handset to the Bell network because it might have a resistance load that might feed into something that might cause a relay to singe once every 800 years, but they had convinced some court that was a problem. So we are not talking about today's world. We're talking about everybody's stuff being proprietary and done by themselves. It was either done by Ma Bell or by the DOD, and so on.

Then other things happened. The DOD decided that it was cheaper to buy computers in bunches rather than per application, because computer hardware was expensive in those days. What happens when you do a fixed-price, low-bid competition is that you get the dog of the week. So we ended up with eighty red Honeywell mainframes. That contract was the only thing

that kept Honeywell in business. We were their last bid. GE [General Electric] went out of the computer business while we were in this time frame. All kinds of people went out of the business. We managed to buy Honeywell. Their operating system had nothing to do with IBM. Their disk drives had nothing to do with anybody else. We got what we deserved. We got a really cheap set of hardware that was useless. But, having bought it, we now set up an entire program called the Worldwide Military Command and Control System information system to build the software to allow these dogs actually to perform a useful function. That's the kind of job that we used to have in ASD(T). It changed its name, but that's a trivial issue.

I was there for the last four years before it reorganized, so I watched Mr. [James R.] Schlesinger's term as secretary and during Mr. Rumsfeld's term as secretary. Neither one wanted us there. When I would go up and see Mr. Clements, who was the deputy secretary, and was the guy who actually made the decisions, he would look at us coming and say "I'm going to get in trouble. Every time you come in here, somebody screams at me right afterwards."

We were discovering the National Environmental Protection Act, which required the government to produce environmental impact statements. We were trying to prove that if we modulated a wire in Wisconsin the moss would not grow on the south side of the trees instead of the north side and confuse the migrating birds. *Sixty Minutes* was all over us every month.

Oettinger: I think it was a sizable chunk of Wisconsin real estate!

Stenbit: No, it was a very small piece. It was about six inches wide and a hundred miles long. In any case, the first time we turned on one of those systems, they rang every telephone in West Virginia, because they used the old rotary dial telephones and every time you got any kind of electric field they would ring. So there were some very interesting problems going on.

We did some very useful things through interoperability. In 1975, for the first time nuclear weapons owned by the Army and the Air Force were fitted with devices that voided their ability to be used unless they had external information. Prior to that time, it was a highly intricate procedural set of controls, but it basically was up to the folks who had them in their hands. I think of that as an enormous stride forward in the balance between "minimizing maximum regret" and still being able to get something done if we needed to. How could we do that? Because we had confidence in the coding, and confidence in some communications systems that actually went worldwide and were survivable, and we converted systems that needed fifty-two aircraft working simultaneously to make them work to needing three, so we saved money and made communications more reliable by changing frequencies and changing the way we communicated.

So there was a lot of integration, if you will, that went on in this particular timeframe, but it was all around special-purpose stuff. Everyone could see that the end of that game was already there: that we were going to be dominated by the commercial world. Even in those days it became pretty obvious what was going to happen. The Carter Administration decided to change how this worked. President Carter said, "All of this is just part of acquisition." That was a mistake, because he missed the policy aspects of that. He took a gentleman named Gerald Dinneen and he said, "You are now "C3" and "I," but you're also the deputy acquisition guy in the department." So he took what were fundamentally mixtures of policy, technology, and acquisition and made them

into an acquisition-focused system, and lost the bubble a bit (in my mind) about some of the more interesting interactions that occurred in those days.

Oettinger: There is an account by Dinneen in the proceedings of the seminar if you want to follow up on that.[5]

Stenbit: I'm not trying to say he did up, down, or indifferent. He was assigned a job, like everybody else.

In any case, that lasted for four years. Then C3I kind of was moved out from under acquisition, and has stayed there ever since. The structure has to do with the policy, and it has to do with strengthening the hand of the secretary to enforce things such as interoperability—to actually stop people from doing things that don't work with other people, et cetera. It's been like that since 1981, so that's twenty-two years. Now Mr. Rumsfeld is back, and he remembers it used to be split, and so he just split it this week. "C3" and "I" have now split.

Oettinger: Is Steve Cambone confirmed as under secretary for intelligence?[6]

Stenbit: He is confirmed as of this morning. All the jobs involving integration of information are still present, and therefore the argument to have an end-to-end purview of what's happening with regard to information sources and information flows is still a very valid one within the Pentagon.

But there's another problem, and that is the alacrity with which the intelligence community serves what is in fact an ever-expanding plethora of requirements from the Defense Department for speed and accuracy and persistence, which are in fact not consistent with sitting in a room doing studies and writing reports. Once again, I'm not trying to be pejorative, but you need to understand that there's a difference. Political intelligence is not, in general, time sensitive. It's more like history. It is predictive. Its utility is to help people understand why other people are doing what they're doing. If you happen to find out exactly what the position of the French ambassador to the United Nations is before the vote next week, it could be tactical, but what good does it do you? If you're a company and you find out what the other guy is going to bid, that's a different issue. You change your bid. So maybe it makes a difference, but it is in fact fundamentally a slower process.

The bottom line here is that there's an enormous pressure to increase the flow of information from the intelligence community to the DOD over paths that haven't been used in the past. One of them is to the secretary, by the way. We have a very interesting system. There are committees that control the priorities within the intelligence community, and on those committees sit the secretary of state or his designee, the secretary of the treasury or his designee, the national security advisor, an Army person, a Navy person, and an Air Force person, but there's nobody there for the Secretary of Defense. So actually, there is physically no voice for the Secretary in the priorities of what gets done. He doesn't like that, to put it mildly. There's a whole raft of

---

[5]Gerald P. Dinneen, "C^3 Priorities," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1982* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-82-3, December 1982), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/Dinneen\Dinneen-i82-3.pdf

[6]Dr. Steven Cambone was previously principal deputy under secretary of defense for policy.

issues about intelligence information flow that Mr. Rumsfeld is worried about, and he believes it's better to concentrate on that and take a hit on the interaction and the interconnectivity than it is to emphasize the interconnectivity.

He clearly thinks the interconnectivity is still important, because he wants the remaining part of whatever (we haven't figured out what my office is going to be called)[7] to emphasize end-to-end information integration, from intelligence all the way up. It's more like a chief information officer role, if you wish, than it is a special-purpose kind of role. So that's the evolution.

The terrorism aspect that you brought up made that all the more complex, because now the interface has to occur with the law enforcement community as well as with the national intelligence community, and that's hard. Those of you who have not thought that through may think that everybody in the government just fights with everybody else, so they don't tell anything. You have to understand: we have a Constitutional problem in our country about the difference between intelligence for national security purposes and law enforcement. They're very different. In the one case, the sanctity of grand jury investigations and the secrecy of the information are in fact Constitutional in nature and the information is not supposed to be shared.

They have some other problems. When prosecutors bring somebody to trial, their information is all subject to discovery by the opponent, so it behooves them not to keep lots of records of alternative hypotheses of the crime. In fact, it behooves him to come to a conclusion quickly about the hypothesis and then build a database that confirms it. That's the opposite of intelligence, where you're trying to search for alternative hypotheses. So there are institutional issues that are very real.

On our side, we are very reluctant to hand information to a law enforcement process where discovery has to do with chain of evidence. The chain of evidence means the lawyers for the defense can go back and find out where we got it. In a lot of cases, we're not interested in telling an open court where we got the information. We have secret systems. We have security systems we built up to attempt to keep some of that secret. So there are real problems that are not computer problems or egomania problems or interoperability problems, but Constitutional in nature, that cause sharing information to be a very tough job.

Oettinger: Before you go on, one other footnote, because adaptation to the issues that John has just mentioned is taking place in a very dynamic sort of way. One of the longest histories of accommodating to these issues is the creation by the Foreign Intelligence Surveillance Act [FISA] of secret courts that have a role of applying Constitutional principles, but in a closed setting, so as to maintain secrecy. If some of you get involved in this area, looking up the FISA court is one manifestation, prior to the more recent enactment of the Patriot Act following 9/11, of adaptations, for better or worse, to these shifting concerns.

Stenbit: That court is set up to protect the Constitutional issues that I just mentioned. You get into the angels on the head of a pin about "If I'm going to go do something, I have to prove it has a foreign intelligence value." If I say it has a law enforcement value, it can't go to the FISA court;

---

[7]On May 8, 2003, the assistant secretary of defense for command, control, communications, and intelligence became the assistant secretary of defense for networks and information integration/DOD chief information officer.

it goes to a whole different court, with a whole different set of procedures. Once I do that, and they give the approval, I am then forced to live under the constraints that come with that, which are severe, about "no American entities" and so forth. So there's a rather intricate set of laws around what I was just talking about.

Student: Who's winning the battles? The civil liberties advocates or the security advocates?

Stenbit: I don't think it's a battle. We're not going to give up our Constitution, so we're going to have a major challenge in this world of bridging how we deal with the subject. It's not an issue in my mind of either side winning; there are just some fundamentals that are really hard.

Student: For example, with regard to facial recognition, the security folks say that we want the cameras to recognize folks so we can see who the terrorists are, and the civil liberties people are saying "You're spying on us."

Stenbit: That's where I was headed. Let me head as close as possible to the law enforcement versus foreign intelligence issue, which is an interesting one. The addition of terrorism forces us to face those issues both inside and outside the United States. But the thing that's really a big deal is that the DOD is not supposed to worry about anything inside the United States. There is a constraint there, namely the Posse Comitatus Act of 1878, and you should be happy that there is such a constraint. It is in fact the DOD's job to protect us from outside threats.

Oettinger: There's an article, if I could put my hands on it, by Stewart Baker on the Posse Comitatus Act. It takes a somewhat different view: that there's ample authority and precedent for military intervention in a variety of domestic affairs that included, for example, integrating the schools.

Stenbit: That was the National Guard. I don't think those were ever active duty military.

Student: A previous speaker from Northern Command told us, "Yes, there is this posse comitatus, but there are enough exceptions that we're not too worried about it."[8]

Student: He actually said that troops were used in the integration situation and in the Los Angeles riots.

Stenbit: All of these things have waiver rights, and they usually require presidential findings of some type. In fact, almost all of these kinds of issues do have waivers that are allowed. I'm not sure of the exact facts, but it's certainly true that they would try to use the National Guard before they would use federal troops, because of the posse comitatus issue.

But at the fundamental level, the DOD operates against foreign threats, and the DHS is supposed to work domestically. The DHS job is a lot harder than ours, because we clearly have a

---

[8]See Dale W. Meyerrose, "Adapting the Military to the Homeland Defense and Homeland Security Missions," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2003* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-03-1, May 2003), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/meyerro\meyerro-i03-1.pdf

decentralized security system within the country, what with all the police and fire and various special services and so on. That's not something that's ever been pulled together particularly well, and that is a big job.

The one thing that we would like not to happen is what happened after September 11. I'm not complaining, and I think it's not inappropriate that what happened did happen, but it was a true change in our assumptions as well. We were about to go to Afghanistan, and we were looking around for all the people it takes to do that. We had 89,000 people deployed in the United States doing things that had nothing to do with the DOD, but we happened to be the only ones around who could stand around with guns in the airports and at border stations and so on. Some of the things we were doing, like flying F-16s and AWACS [Airborne Warning and Control System] and so on were a little more specialized toward the DOD, and in fact we have the role of protecting against enemy aircraft. We never thought those aircraft would be flown by American Airlines.

So lots of changes have occurred, but I would say to you that the kinds of problems that I have about integration of information within the DOD are absolutely trivial compared to those of whoever is going to have that job in the DHS. It's going to be a very tough problem.

Oettinger: To underscore this, he's dealing with three services and twenty-eight agencies, but it's a two-digit number, as opposed to three-, four-, or five-digit numbers in terms of the jurisdictions and responsibilities involved in that fragmented homeland security environment.

Stenbit: One of the things that I worry about is that the DOD has been asked to be the executive agent for a lot of national things. One of them is the National Communications System [NCS], which has to do with how communications are provided not for the DOD, but for the nation in certain cases. For instance, there's a system for senior government officials so that when all the phones jam up on Mother's Day, for example, we have a system that gets around that. It's called GETS [Government Emergency Telecommunications Service]—GETS gets around it. On 9/11, the cell phones all blocked up. We've had, in the same NCS, a proposal on the table for quite a while about how to unblock cell phones for privileged users. That now exists in three cities in the United States. The DOD is not going to do that anymore, because NCS has transferred over to DHS. Since that was done in the DOD as sort of an incremental additive to all the stuff we were already doing, I think it's going to be very hard for a long time for those functions to be done in DHS. There are some interesting issues wrapped around what you asked, not only on the intelligence side, but also on the communications side.

Oettinger: It was created during the Kennedy or Johnson administration.

Stenbit: But it was really reenergized when Judge [Harold] Green broke up Ma Bell in 1982. All of a sudden, in a heartbeat, we had to be able to negotiate with multiple vendors in a legal way to create networks when a disaster strikes. For instance, rebuilding the switches in Lower Manhattan was entirely done by DOD folks through the NCS kinds of mechanisms, although it was done for FEMA [Federal Emergency Management Agency] and FEMA paid us. That could not have been done without this infrastructure that's been around for a while.

Oettinger: This was augmented by the National Security Telecommunications Advisory Committee [NSTAC]. It's an interesting trend, because the NCS was sort of a paper tiger. Then

the NSTAC brought in the chief executives of the increasingly fragmented telecommunications industry, and over the last couple of years people from the computer industry and the networks were generally brought in as well. So the solutions to this problem are not exactly right there, but they're working on them.

Stenbit: There are twelve outreaches from the DHS to industrial groups for critical infrastructure protection. One of them is telecommunications. That exists in the NSTAC. It's the only one of the twelve that works. The other eleven—finance, food, energy, chemicals…pick the twelve sectors that represent the basic economy of the country—are pick-me-up teams that are trying to figure out when to have a meeting and who's who.

Oettinger: Each of them has an Information Sharing and Analysis Center that is supposed to coordinate among the various elements of these industries within which the competitors won't give each other the time of day. There are many unresolved issues.

Stenbit: I'm going to stop there. I could keep going, but it's not my job and I'm happy I'm not over there.

Let's chat a bit about the issue of the budget and the CONOPS and the n^2 to n. I talked to you a bit about how twenty-five years ago we were doing TRI-TAC [Tri-Service Tactical Communications Program], which was trying to superimpose a 16-kilobit voice standard on everybody, and basically built these big interoperability machines that cost an awful lot of money. Nobody wanted them. They didn't work very well. They were always late. The software didn't work. It was a typical government program. Ultimately, though, had there been a war in Europe, that's what would have been the glue that held everything together.

Student: Didn't it get unglued in Desert Storm? When I started with the Air Force, that stuff was still around.

Stenbit: I was going to say that we had started down the cell phone world by Desert Storm, but we clearly hadn't facilitated the whole place, so it was a mixture of the two.

Student: Was that the STU-III [secure telephone unit]?

Stenbit: No, STU-III is a wire-line system. It has nothing to do with this. STU-IIs were 2.4-kilobit systems. That was a different idea. Then we were in the world where AT&T had been broken up and you could add stuff to the net, so now what we needed to do was produce our own fancy handset, compared to somebody else's handset. We had some solutions that we could use, other than the ones that were prescribed before Judge Green.

In any case, I was talking about 1975, and I would assert that, in those days, like the Athenians when they were fighting Sparta in 1000 B.C., we in military operations were forced to be synchronous in space and time. Let me chat about that for a second, because I think it's a big-picture principle. We were forced to be constrained in time because everybody had to be in the same place at the same time in order to have a fight. Think of World War II movies, with the Navy battleships lined up off the coast of the invasion beach going "One, two, three, NOW!"

WHAM! All the shells go. "Okay, one, two, three, NOW!" *WHAM!* All the shells go. That is my definition of synchronization in time and space.

We were synchronized in time because we were in a switched telephone world that was run with *erlangs*[9] and calculations and so on—a decidedly smart push world. Anybody who knew anything needed to know the total state of the universe in order to figure out whom to tell—or to push it to. When the captain of the *Pueblo* was captured, if he had only known the phone number of the Marines in Okinawa it would have been over in half an hour. But what process would he ever have used to know the phone number of the Marines in Okinawa? I would assert to you that it was an impossible problem. It was made even more impossible by the fact that whatever radio he had would have been different from whatever radio the Marines had.

That's what this n^2 issue is. To have interoperability, if there were n different devices you needed to have n^2 solutions. Each one had to have a solution. I guess it's really n times n–1, so I'm off a bit. It's on the order of n^2. (I'm a Van Gogh person, not a Norman Rockwell person. What's a factor of n here and there?) We were forced to be synchronous in time, because if somebody called you and you didn't answer, nothing happened. We were forced to be synchronous in space, because basically we didn't know whom to call, other than the ones who were on the little plastic sheet we had in front of us. So while you could be anywhere, you had to stay in the same place or else nobody would be able to catch you. That was really what TRI-TAC and some of these other systems were trying to fix—to allow the logical equivalent of telephones to move in the battlefield and be useful. Certainly we never were able to connect aircraft, other than in the most rudimentary of possible ways. We never could correlate where they were with what we were saying, or anything else. That was just impossible.

That has an implication, and it is that a guy named F.W. Lanchester, a British engineer of the late nineteenth and early twentieth-century wrote some stuff (you probably know this better than I do, and I fully accept that if I'm off you'll help me) that basically said that in a military engagement, whether it's the Athenians and the Spartans or 1900 or the mid-1970s, the defense has an advantage over the offense of three to one.[10] It worked out over time. There were deviations from that. This assumes they were more or less equally matched folks. If the longbow comes out after the French horsemen, and there's a technological leap, it doesn't work, but after it balances out again it's a three-to-one kind of problem.

Why does that happen? It's easy. I don't know why it's three, but I certainly know why it's an advantage: because the defense gets to choose the place. Unless they're stupid, they pick one that's good. They also have the smallest internal lines of communication, so they can communicate better, by definition. The bottom line, after you've wrapped all that together, is that it's about three to one.

---

[9]An erlang is an international unit of measurement for telephone use, equal to one caller using the telephone for one hour.

[10]See J.G. Taylor, "An Introduction to Lanchester-Type Models of Warfare," in *Modeling and Simulation of Land Combat*, L.G. Callahan, ed. (Atlanta, Ga.: Georgia Institute of Technology, 1983), 34–66.

What do we do today? It's about a 1000:1 in favor of the offense. In the first Iraq war there were 300 casualties on our side versus 300,000 on theirs. In Afghanistan it was 100:1 in our favor. Combat efficiency: advantage to the offense.

Student: Aren't you talking about a technology difference?

Stenbit: We've been doing better than Moore's law for the last twenty years,[11] according to our productivity measure. (Unfortunately, our productivity measure is how many people we kill.)

Student: You're not comparing equally strong adversaries.

Stenbit: I'll challenge you in the following way. We have an all-volunteer force. That's part of the strength. We have stealth, and GPS [Global Positioning System]. I would assert to you that if we had all of those, without one other element, we'd still be in the Lanchester's law regime. We might have shifted it from a factor of three to the defense to a factor of three to the offense because we could shoot further or something like that, but fundamentally I will assert to you that the real difference is that we went from a smart push telephone system, where somebody who knew something had to know to whom to tell it, to a broadcast system, where anybody who knows something puts it on a broadcast system without knowing where it's going. So, instead of being forced to be synchronous in space and time, we are now forced to be synchronous only in time (because we only send it once), but we are asynchronous in space. We can be anywhere we want and we can get the information arbitrarily, and the person who's sending it doesn't need to know anything about who's receiving it. So it's a smart push world that has broken the paradigm that the only person who can shoot something is the buddy of somebody who finds it. He's already on the list. I will assert that is a very large part of our ability to apply the technological resources we have in the flexible ways we do to change the ratios as well as we have.

That's where the boss's favorite story comes from: the one about the guy in Afghanistan on the horse with the wooden saddle who is able to call in a B-52 JDAM [joint direct attack munition] that had flown all night from Missouri. He didn't do that. In the old world he would have had to do that; he would have had to call the B-52, but he wouldn't have known the phone number. In the new world, all he had to do was say "XYZ coordinates, get it on the broadcast," and the guys who were out there who could attack X, Y, and Z had a conversation and said, "Okay, I'll do it." *BOOM*! That's a very, very different world. That's also a very different world in the interoperability business, because it's an n problem, not an n^2 problem.

Oettinger: Let me ask you a question there that I didn't have a chance to ask over lunch. Obviously, only needing n things is a lot cheaper and easier than having n^2 or n times $n-1$, but it also implies in a naïve way that there is a central node that then becomes a very attractive and vulnerable target as distinguished from the inherent robustness of n^2 connections. Is that correct? How do you work the tradeoff?

[11] Moore's law states that the power of new information technology will double approximately every eighteen months.

Stenbit: That's correct. It turns out we do that by not having any one central place, because all the networks are different, and all the broadcast systems go different ways. I think there's a case of advantage through distribution, as opposed to somebody trying to do that all in one place, which would be wrong. We do have something called the Global Broadcast System, which is a single node, that most of this stuff goes over.

Student: My interest is in computer security. When you describe this guy on horseback putting out coordinates, how do you verify those coordinates? What happens if they are intentionally a digit off, which causes the bombs to fall on allied forces? We had a bunch of friendly fire incidents in Afghanistan.

Stenbit: For exactly that reason. He put the wrong GPS coordinates in.

Student: But we believe that wasn't intentional.

Stenbit: These are encrypted.

Student: Yes, but you're thinking of communications intercepts on line. You could have somebody there holding a gun to the head of the guy on horseback. You could have a guy who was a plant from a sleeper cell. What are the protections?

Stenbit: The malicious insider is a very serious threat in all cases. In a broadcast case, it's not as bad, because the wherewithal to be a broadcaster is actually quite expensive and complex. The enemy might be able to find somebody, but the ability exists to find out in a very short period of time whether that person is real or not, because his boss is going to start asking him to do things that he will not be able to do. There's a certain "connectivity into the force" kind of issue. Just picking up a crypto thing won't let somebody make it work, because there's a whole bunch of other protections. You can change it by the day, the hour, the minute, or the session. It depends. We balance those kinds of issues against risk.

Let me stick with this issue of being in a broadcast mode, because that's what goes on today. What happens is that we have created a lot of stovepipes, because we've told professional people that it's their job to create the prioritized stuff that goes on their broadcast. We have told NIMA [National Imagery and Mapping Agency], "You build the business process that fills up the picture broadcast with the best pictures first and the worst pictures last. That's your job, and please do that." We've told NSA to do the same thing with their stuff, and we've told JSTARS [Joint Surveillance Target Attack Radar System] to do the same thing with their stuff, and we've told AWACS to do the same thing with their stuff. When I was over in Afghanistan and Qatar and Kuwait a month ago, everywhere we went we found a place, whether it was a tent or a Quonset hut or whatever, where there's a tier of people in a very large room with big wall screen displays, surrounded by about another thousand people on a local area net, all of whom are connected to about a dozen satellite dishes in the back yard, all looking at these networks.

We have gotten pretty adept at building what we call fusion centers. They are places where you've got to record the broadcast, because it only comes once, so we're still synchronous in time. We do it at the time that the bureaucracy chooses. We are asynchronous in space, because we can now do it virtually everywhere in the world, as long as we spend the money to build the

antennas, the network, the storage, and the GCCS [Global Command and Control System]-compatible software to be able to fuse it all together. We can't share it with anybody, because it's too hard. The security to bring in a Brit or a German or a French person, or certainly a Pakistani, is just too hard, because the information is now at such a sensitive level that it's very difficult to share with anybody who is not "in the club."

We have a system that works very well, but we're spreading ourselves out in smaller and smaller groups. That doesn't bode well for a system that costs a lot of money to be able to cross-strap the information from all of these systems. You've got to bring in a lot of satellite dishes and other things.

Student: When you say it's very difficult to share all this information with the foreign services, is it just because it's unfiltered as it comes in to you, so you have to filter it before you send it to them?

Stenbit: It's a classification issue. It's that you are getting so much, and it exposes so many things, that once you let them into this enormous flow there's no filter. So you have to decide that they either get everything or they get nothing. We generally choose that they get nothing until that gets too problematic, and then we let them see everything anyway. That's not a very good system, to my mind.

Oettinger: Maybe this occurred before the period you're describing, but General George Joulwan, after he was CINCEUR [commander in chief, European Command] and doing Bosnia and so on, described tactical sharing of intelligence with Russians, Germans, and so on, who had an interest in keeping from shooting each other or in alerting each other that some Serbian character was going to pick them off. Is that apples and oranges?

Stenbit: I personally had to go and make sure that the Russians in Bosnia were getting our very best overhead photography. That was a bad choice of person to send, because I had a very hard time with that. In fact, it's what I just said. You say no, then you say no, then you say no, and then it becomes untenable and you do it—and you do it without any modulation, because there's no way to modulate it. Once they're on the broadcast, they're on the broadcast.

It turns out that in that case we left them on only one broadcast, which was the picture broadcast. We didn't let them have anything else. But it could have gotten to the point where they had everything. They do a better job of intercepting than we do, and we didn't get their stuff. The French were there exploiting the system. They had the best people I've ever seen pulling down every picture, but they weren't interested in the pictures. They were interested in figuring out what was taking them.

Student: You said that it's sort of binary. You say no and they get nothing, or you say yes and they get it all, at least for the entire process.

Stenbit: I overstated.

Student: Even compartmentalizing to say they get all of Type X, why can't you create a hybrid system, where U.S. forces are on the broadcast, but then if you want to tell anybody—say a

Russian force or another NATO [North Atlantic Treaty Organization] force—you just go back to the old system and pick up the phone. You go back to the old pushbutton.

Stenbit: It turns out that's not diplomatically acceptable. There is no question that they know that kind of stuff and don't like it. There's a lot of pressure. You can do certain things. You can look at the picture before it goes on the broadcast, and say, "Hey, wait a minute. This actually is a little different from some other pictures, so maybe I won't send this one." You end up self-censoring for both your own and other forces.

Student: I've been on several joint task forces where I was in the joint information operations center. We actually had situations where we had U.S.-only rules. Then there was whatever country we were exercising in.

Stenbit: In which case you'd have a different broadcast. If it's a single country it's not a problem, but there are fifty-two people down there in Tampa, and the number of common security levels is zero. Once you go down this path it turns out to be very difficult.

Anyway, my point wasn't to get bogged down in that. It was really to say that because we have caused ourselves the problem of making ourselves synchronous in time, it forces us to incur a lot of costs to make that system work. It means we have to store all the stuff that is broadcast, whether we're using it or not; we have to go through it to make sure it's what we're interested in; and then we have to fuse it from the various different broadcasts into something useful. We have a system we do that with, called GCCS. It works very well, but it has these awkward sorts of issues.

We have the other problem that we're still bound by the transmitter's perception of what's interesting. One of the other things that comes up in all after-action reports is "The data were there; they just weren't in the right place at the right time." That's another way of saying that the brilliant pushers were wrong about what they were supposed to be pushing at that particular moment.

Oettinger: In terms of some of the points I keep trying to make to the class, there's another sort of unresolvable balancing act here. In total demand pull, the demander has to be enormously versed in what the possible sources are. He has to know what to ask for, and there's so much out there that he'll never live long enough to get it. You then revert to somebody out there picking it and pushing it, and that person is going to push it wrong. If that analysis isn't off the wall, what are your criteria for how you balance this?

Stenbit: You've certainly got me going in the direction in which I want to go. I want to go to smart pull. Let's talk about that. There are some implications about smart pull that we have to solve first, and there are some benefits. Then let's talk about the problem you just talked about.

First of all, the reason I'm in smart push is that I'm bandwidth starved. Even though I've got seventy people looking at the same picture, I'm only sending it once. So if I'm going to go to smart pull instead of smart push, I've got to fix the bandwidth problem, and that's why I'm happy somebody asked about bandwidth. If I've got seventy people, and they all pull the same thing at the same time, I've got to have seventy times as much bandwidth to have the same system work.

Student: You can cache it.

Stenbit: Then you're stuck with the same kinds of timing issues.

Fortunately we have available to us a technology that allows all of that, which is called lasers, fiber optics, and lasers in space. We can make quite a dramatic jump in bandwidth from the RF [radio frequency] world. So we have in our hands the opportunity to basically change the bandwidth limits instantaneously by about a factor of 1,000. That's a pretty good start.

That allows us now to be in a smart pull mode, but that's useless unless we change the stovepipes that are doing the processing. It won't improve if they still do what they were doing before, which is that they decide what comes out in what order at the end of their process. That is called TPED in our world—task, process, exploit, disseminate (disseminate being at the end). We have to get rid of that. We now have to change the business process of the generators of the information to task, post (for everybody), process (in parallel), and use (in parallel).

Say we're now back to the picture guys. They're going to have a business process where they take the first picture that comes off and do some quick analysis about where it is and whether the clouds are there and put some metadata on it. From that metadata they decide if it's a high-priority picture, and if so, to whom they send it (because there's an expert in trees and an expert in sand or whatever). They do that at the front end of the process. That becomes the beginning of the queue of the automated business process.

I come by and say, "I want you to post all of that on a smart pull net at the same time that you put it into your business process." I now want amateurs to be able to pull the raw data before the professionals get their hands on it. In so doing, I've broken the time constraint.

If I'm now in Afghanistan, I know my pictures are going to be last, because Iraq's going to be first. That means it's hours, if not days, before I get the picture. But I've been told to go over the hill today, in the next two hours. In the current system, I can't do anything. It may be interesting to me when I get the picture three days later, but it doesn't do me any good because I've already gone over the hill. That's what I mean by the tyranny of time synchrony and why, in my mind, the parallel and smart pull is the issue.

Now, I accept what Tony said. There are a lot of penalties that go with this if it is used incorrectly—and I will guarantee you that there will be some people who will use it incorrectly. However, there are also a lot of people in my world who will have their lives saved and will inflict even more damage on the other side, because they have had the opportunity to break this time synchronization problem.

Oettinger: Every grunt being a photo interpreter?

Stenbit: You got it!

Second, the facilitation that's required for somebody to use this information at the edge of a wideband network is a dumb terminal. You can put the processing on the network. So I've removed the other problem as well. I can now arbitrarily have as many people as I want gain

access, instead of just the ones who can afford ten satellite antennas, all the high-speed processors and storage they can find, and a big LAN [local area network] with 1,000 people on it.

To get to the earlier question, there's a third thing that happens, which is that I can now audit individually who gets what and who pulls it down, so I have a whole new mechanism of risk management. I can now afford to let you have access to information and tell you, "But don't go to the following servers, because if you do I'll put you in jail." I can now audit whether you obey or not. The first time you go someplace where I don't think you should go I can change your access. So I have a dynamic access control ability. I have a lot better information assurance [IA], because instead of 5 million people with fat clients at the edge of the net being able to become insiders, I now have 4.95 million people at the edge of the net who have dumb clients. If they're really good at typing they might be able to do something, but they can't do anything else. I also have 10,000 or 15,000 administrators whom I have to watch out for, but that's a lot easier than 5 million people.

So I've changed my IA problem. I've changed my dynamic allocation problem. All I had to do was change the bandwidth by a factor of 1,000, make it end-to-end interoperable and seamless, develop IP-based encryption instead of link encryption, get a gazillion dollars, and keep the Pentagon going in the same direction for about ten years. That's an outline of the revolution that I'm attempting, and we can talk about that later.

Oettinger: Isn't there a lot of artificial intelligence in there? You're assuming that those dumb terminals have a lot of stuff in them that will convert that stream into something that ordinary human beings can comprehend. Or are you assuming all sorts of specialists?

Stenbit: I grant that there will be value-added suppliers on this network, just as there are in other networks. I don't have any problem with that. When people talk to me about "publish and subscribe," publish is fine. That's really what I'm talking about. A lot of people say, "Look, I'll tell you what you want. All you have to do is fill in your profile." That's a surrogate for making me a smarter pusher, but the fact is that you didn't exactly predict what your profile was on time, because you got a different job the day afterwards. I think it's fundamentally closer to my definition of an appropriate program, which is that it minimizes the maximum regret as opposed to optimizing the output.

What happens in the world I'm talking about is that you get a lot of collaboration at the edge—power to the edge, in this particular case. It changes command and the definition of command mightily, because it now becomes selection among alternatives that have been created by people whom you've never met, as opposed to sitting around in a room with your buds and deciding what you're going to do and then telling everybody. But in my world, all the people who have guns could spend twenty-four hours a day optimizing what twenty things they can shoot, because they'll have the same data anybody else has. I don't propose that they shoot all of them. I think there are rules of engagement and a whole bunch of other stuff, but it's a very different world.

But I have to do two requirements. First, I must change the business process. Actually, the enthusiasm with which NIMA and NSA are getting at the change in the business process is quite high. It's very interesting, because it's happening anyway. In the NSA, for instance, you can't get

anything today until it gets through their business process. It won't come out. Their business process includes translating into English, but almost anybody who has a real problem happening someplace else has somebody around who speaks the local language, and who probably would do a better job of translating into the context than the theoretician who is reading it wherever the heck he or she is. The users also get it late, because they have to wait for the English translation. So, Mo Baginski[12] says, "Hey, I've got to get with this program of posting in parallel, because there are a lot of people who will take it down to the native language." Think about it. She doesn't know which analyst to send it to, unless she's done enough of the data or metadata to decide if it's in Urdu or Farsi or whatever. So I'm not talking about doing extra stuff in addition to what she'd have to do anyway for her own internal business process.

Oettinger: You've raised a point that, assuming for a moment that everything you describe works, brings to the fore that the chain of command, the chain of information flow, is going to be different. People are not historically used to the notion that those are separate. What you're saying is that you can have full knowledge. In principle, the grunt now has full knowledge, as much as the general—probably more, because he's more computer adept. Now you have to establish a rule system—rules of engagement, positive control, whatever you want to call it—that deconflicts the twenty various people who might see the same thing and might all get trigger happy, or end up not paying attention, depending on which view you prefer. So that's an issue that has been so academic in the past that nobody has paid much attention to it.

Stenbit: It gets to the issue about how JFCOM actually operates in testing new TTPs—training, tactics, and procedures—and rules of engagement. It's not in the PPBS, but how do we in fact evolve as we get to be more net centric?

Let me assure you that what I'm talking about is already happening today. It's just happening in this funny broadcast mode that I'm talking about, and so it only happens in a very few places. NIMA today has a link directly to Tampa, and the people in Tampa are able to pull all the pictures that NIMA processes before the NIMA analysts have necessarily looked at them. NIMA sends people to Tampa, so they're not amateurs. Jim Clapper has taken on the job for me of helping to define the software that I put at the edge of my network.[13] It's better than PhotoShop, and it allows people to do some image interpretation. We do not intend to have them do mensuration, because that's a pretty hard problem.

General Hayden[14] and I agreed that what he should do first is translation for "gisting" purposes, so that somebody gets enough of an idea of what the thing says that they can get excited about it (or not), even though it's not a perfect translation. We are working the problem of "If we have such a network, how would we facilitate it to make the amateurs less stupid?"

There are some other issues that are very important. This network has to have data standards. I'm going away from an application interoperability world into a data interoperability world, and I'm counting on IP and TCP/IP, and so on. At my level of interoperability, I'm getting

---

[12]Maureen Baginski is the director of the signals intelligence program at NSA.

[13]Lieutenant General James R. Clapper, Jr., USAF (Ret.), is the director of NIMA.

[14]Lieutenant General Michael V. Hayden, USAF, is the director of the NSA.

out of circuits. That means radios are different, and modulations are different, but it doesn't mean you can't do it. It does mean the cryptos are different. We've got to work on that. What's also interesting is that we need a data standard that's different from the standards that commercial guys will have.

For instance, we need pedigree. Let's go back to the picture and the guy in Afghanistan. I now have my system to get to whomever anywhere in the world, and it extends not only through the ground but also through radios. The guy pulls down a picture, looks at it with his PhotoShop Plus, and says, "My God, there's a tank on the other side of that hill I'm supposed to go to. I'm going to change my plan." He sends an e-mail to his boss, and that gets posted on the same net.

Let me tell you: one of the big asymmetries today is that the operations guys share less information with the intelligence guys than the intelligence guys share with the operations guys. This is an asymmetric problem, and it's going to have a lot of fights associated with it—no question about that. So he posts "If anybody's interested, there's a tank on the other side of this hill." But it's also posted that he's an amateur. He doesn't have any pedigree as an image interpreter.

Now we're back at NIMA, and Sam, who's the image interpreter, finally pulls up the picture and looks at it, and he says, "Hey, Tony! You know those wooden tanks? I found them! I've been looking for them all week, and they're right over on the other side of this hill." Now he publishes a document with a pedigree of professionalism, and I'm very willing to allow that the average NIMA person is a better photo interpreter than the average grunt. I'll even give you several sigma.

I now have to go back to the data that I posted, find out who pulled it, assume he's an amateur, and send him an e-mail saying, "Dude, somebody who knows what they're talking about has taken a look at this picture, and you might want to go take a look at what he said." So I buy that I have some constraints in this network that I have to provide or I can't do this security business that I have to enable anyway.

That leads me to interesting questions, such as "What is this data format? We're building this network right now, so we've got to get with this program or we're not going to be able to do it. When do we go to IPv6 [Internet Protocol Version 6], instead of IPv4? Is IPv6 going to help me with this, or hurt me?" My answer is that we've got to go to IPv6, so anything that comes after 2008 has to be IPv6, but we can't do it now. We're going to start assuming that, but I've got to get up my courage to write that down as a DOD standard. Well, that means that I've probably got to stop buying anything that doesn't work with IPv6 today.[15]

So there are very interesting issues going on with this program. But let me make sure that you do understand that we are embarked on this next revolution, which is to go from broadcast circuits to network centric smart pull, for the reasons that I tried to explain. You're very good, because I knew you were going to ask the questions that would let me give my speech anyway.

---

[15]On June 13, 2003, Mr. Stenbit announced the DOD's implementation of IPv6 by 2008. The transition from IPv4 to IPv6 will phase in, requiring network capabilities purchased after October 2003 to be both IPv6 capable and interoperable with the current extensive IPv4 installed base.

Student: Are you going to take in the tactical intelligence too, to get the real-time video?

Stenbit: Absolutely, but it goes the other way. The Joint Strike Fighter has the best radar in the world. Seven Joint Strike Fighters are equal to one Global Hawk in terms of square miles per day and high-resolution SAR [synthetic aperture radar]. We're going to buy 3,000 Joint Strike Fighters and we're going to buy 25 or 50 Global Hawks, or some number like that. Seven times 25 or 50 is a lot less than 3,000. You cannot assume, in the world where we're headed, that you can predict the source of information with enough certainty that you can build a broadcast system in advance. That's the other reason not to do it. We're still in the *n* world: all I have to do is get to the network. I have to get to the network whether I'm pulling, pushing, posting, or whatever.

Student: The problem I see with your example is that when it's getting back down to the person sending the e-mail back down to the grunt, he's not sending an e-mail, he's posting something.

Stenbit: No, in that case it's smart push. It's brilliant push, because I know what IP address pulled the picture, so I send it to the IP address.

Student: Isn't that an extra level of effort?

Stenbit: Of course. But it's not that hard. I'm going to record that anyway for my own security purposes, because I want to know if somebody's doing something they shouldn't. Mr. Regan almost got the electric chair the other day for spying, because we knew what pictures he was pulling down from Intelink, and when.[16] That's what went into the court. He had a job to do X and he was doing Y. I don't know if you guys read about this up here, but we convicted a spy the other day in Virginia. It was one vote off from the death penalty. It was an open trial.

Oettinger: Let me be professorial for a moment, at risk of belaboring the obvious, but that's what I get paid to do. You have just had the benefit, over the last fifteen minutes or so, of some marvelous exposition of the interaction between technological innovation and doctrinal issues. I couldn't have conjured up anything better than what John did. Reread Van Creveld now and put his remarks in that context of the ongoing revolution,[17] because you guys are the ones who are going to have to bring this to a conclusion. We're not. But it's an amazing introduction.

Stenbit: Picture why I was cynical about Gerry Dinneen's decision that this was an acquisition issue. I did not describe an acquisition issue to you; I described a revolution that's just as large as the revolution we had when I was there the last time to move us to broadcast instead of switched telephones.

I can tell you all kinds of stories about "once you do it for them they won't use it right." My favorite story is that the very first broadcast system we built was for a command and control chain in 1976 for evacuating Lebanon. We had this single-channel, push-to-talk radio that worked voice, and the lieutenant on the LST [landing ship, tank] and the admiral in Naples and the admiral in London and the general in Stuttgart and from my point of view the chairman of the

---

[16]Brian Patrick Regan was convicted of spying for Iraq, Libya, and China.

[17]Martin Van Creveld, *Command in War* (Cambridge, Mass.: Harvard University Press, 1986).

Joint Chiefs of Staff and the deputy secretary of defense, whom I was watching, were all on this channel at the same time. Everything was going pretty well. We had all kinds of troubles right before that. A lady came down the beach with a dog in her arms, and this whole place locked up about whether or not the dog could get on the boat. Should the chairman of the Joint Chiefs of Staff and the deputy secretary of defense be arguing with each other about whether the dog should get on the boat? The answer is of course not, but if you give people the opportunity to have a new technological toy, they will misuse it instantaneously.

Our current version of that is videoconferencing. Videoconferencing is so pervasive now that we have videoconferences with 500 people on them. The problem is that the big guy's job is too hard for him, so he goes back to when he was a kid and starts mucking around with the job that's not his anymore. All of those things happen. It will happen in my network.

Oettinger: It will always happen. For those of you who would like to study that, there is a long record in the seminar proceedings going back to Lyndon Johnson's famous 8,000-mile screwdriver, when the president of the United States was in the Situation Room doing this kind of tactical stuff. But the interesting thing you'll find in accounts by General Stilwell and General Cushman, and several others, is that eventually folks developed, as in everything else, measures and countermeasures. It was a dynamic issue. MacArthur pretended his teletype didn't work, and so he ignored messages from Truman, and eventually Truman fired him. So you get a sense of the dynamic of this, and it recurs. After the 8,000-mile screwdriver, the folks who handled the Korean tree-cutting incident had insulated themselves and essentially created a network and wouldn't listen to Washington.[18]

Stenbit: That's not true. That is absolutely not true. I had to do that. We had to have real-time TV of the cutting of the tree brought into the Pentagon for the deputy secretary. For those of you who don't remember this, Panmunjom (also a place where I've been that I would not recommend highly) every so often was the location of some sort of nasty stuff that the North Koreans did. It turns out that some Americans, well on the South Korean side of the line, had a sight-line problem between two guard towers, so they went out to trim a tree. The North Koreans came across the line, grabbed the axes, and murdered all four of them. They shot them and then they used their own axes to hit them in the head. It was a rather flagrant demonstration of resolve, or whatever you want to call it.

---

[18]For accounts of the tree-cutting incident, see John H. Cushman, "C^3I and the Commander: Responsibility and Accountability," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1981* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-81-9, December 1981), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/cushman\cushman-i81-9.pdf ; Richard G. Stilwell, "Policy and National Command," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1982* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-82-3, December 1982), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/stilwel\stilwel-i82-3.pdf ; and John Grimes, "Information Technologies and Multinational Corporations," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1986* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-87-1, February 1987), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/grimes\grimes-i87-1.pdf See also John K. Singlaub, *Hazardous Duty: An American Soldier in the Twentieth Century* (New York: Summit Books, 1991), chapter 12.

We were not in any position to go attack the North Koreans or do anything nasty, so we decided we were going to cut down the tree, not trim it. This became the entire operation: to cut down the tree. We put live video into the Pentagon, with maps of where the cutters were, and the covering fire for the cutters, and what we were going to do if the Koreans came. That was a very well-orchestrated attack on the tree. If you go to Panmunjom, there is a marker that commemorates the tree. It is right there. It's easy to see. I'm sorry that you didn't all know about that. It was in 1976, right before this broadcast net was set up.

Oettinger: Don't rely on my fallible memory. Some of the participants in this are on the record, and it's a story worth piecing together.

Stenbit: We did the same thing. We had a ship called the *Mayaguez* captured by the Cambodians. Several things happened in that particular exercise that were pretty nasty.[19]

But from the communications standpoint it was very interesting, because there was an official command system that went from Washington to Hawaii to some place in Thailand to some C-130 that was on the western side of the island where all these people were. The Navy, in the spirit of togetherness, decided to run its own back channel so that the chief of naval operations would know things before the chairman of the Joint Chiefs, and that ran from the ships that were observing what was happening on the east side of the island and went down to Australia and got to Washington. Data from the Navy got to Washington before the data from the normal chain of command, and said, "Everything is great. No troubles." On the other side of the island, the data were coming back, "Forty-three people are dead, it's going poorly, we need to do…." Those data got to Washington about an hour later. This caused all kinds of social problems. But there's a case where we were locked into time synchrony based on where we were and what the paths were, even though they were both dedicated circuits. It's just a problem of communications. We managed to screw up a lot of things in those days, and all of those things are sort of on the record.

Oettinger: Have we gotten through all the questions?

Stenbit: Somebody wanted to know about the TTIC, and the answer to that is "I don't know." So that's easy.

Student: I have a quick one: what is your opinion of the Navy–Marine Corps Intranet?

Stenbit: It's a noble experiment. The Navy and the Marine Corps have decided to outsource 400,000 seats. That's a rather large contract. The good parts of that are that they'll have a better financial plan to refresh technology, they'll have better integrated security, and they'll have some discipline in applications if they ever get it deployed. But it's a hard problem, and it's very difficult to do. They didn't start very well, but I think they're a lot better today. Today it looks to me like a normal program: it's got lots of problems, they find them, they fix them, and it costs money. Actually, at the beginning of that contract, the payments to the contractor were absolutely

---

[19]For an account of the *Mayaguez* incident, see Raymond Tate, "Worldwide C^3I and Telecommunications," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1980* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-80-6, December 1980), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/tate\tate-i80-6.pdf

independent of any progress on the program. It was done by time, and it wasn't coupled to events. That's not my view of a beauty contest winner, but it's not like that anymore.

Student: Getting back to your example of the Joint Strike Fighter and its radar, and connecting it all to get images and that sort of thing, could you apply the example to the concept of the network and having the broadcast where everyone just needs to get on the network? How do you get the services to procure things that talk to each other and that can get on the network? What ideas would you have for compelling the services to produce systems that talk to each other and get on that same network? Is it back to the PPBS cycle, and maybe the role of the JFCOM?

Stenbit: There is a document that the acquisition guys do not like, called the C4I [Command, Control, Communications, Computers, and Intelligence] Support Plan. You cannot get a program through the acquisition process without having produced one. It was during the Joint Strike Fighter acquisition that they started talking about that and about where they have to define their cross-dependencies. They managed to leave out that they had any data links, so they didn't get through the process without adding the data link. It's that kind of a system. You put a regulatory regime in that causes somebody to create enough information so that somebody else can make a decision about whether that's the right way to go.

Now, they don't have to talk to everybody else. All they have to do is get onto this network. So there will be a Global Information Grid [GIG] standard and if they can get onto it they will. I think they think they're going to use Link-16, but they're going to use the Joint Tactical Radio System, which is going to be an embodiment of a Link-16 for a while, retrofitted, but will have a forward-looking network capability. So there's lots of technology, and we could have talked about that. It's actually more fun to talk about how lasers work and how we're going to do all of this stuff, but I think that's for another day, probably not even for this course.

Student: Something that came up in the lunch discussion and actually was a major part of our reading in Ken Allard's book was about service autonomy stovepipes and things like that.[20] The reading makes a big deal about how this is all so traditional, which gives me the feeling that it's kind of path dependent: we've always done it this way, therefore moving away from service specialization is hard, because of this tradition. Do you see any point in the future where the cost of having an OSD apparatus that is constantly running around making sure that people can talk to each other, or use the same hardware or ammo, is outweighed by the losses that would be entailed in terms of special capabilities that come from that stovepiped system?

Stenbit: To begin with, remember that the Pentagon is fundamentally flawed before you start. The National Security Act of 1947 established a secretary of defense who has no money. Zero. Each of the three services (or four if you want) and these days twenty-eight agencies is appropriated money independently by the Congress. So even if the secretary of defense went over to the Congress, having forced them all to be perfect in their budgets, going through that particular process would not have them be perfect in the budgets when they came out.

---

[20]C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven, Conn.: Yale University Press, 1990).

Oettinger: He's describing Harvard University right now.

Stenbit: That's right. You have central fundraising. It's okay to bring money in, but you can't spend any if you're the president of Harvard.

It's a matrix, which, as I described at lunch, is like a law firm where the lawyers have to go to court and win cases on the basis of what the research associates did, because the research associates got all the money and the lawyers had nothing to do with what they researched. That's what happens. If you're General [Tommy] Franks, and you're being asked to go tackle Iraq, you get to do that with whatever the heck the secretaries of the Army, the Air Force, and the Navy chose to buy. So we have a matrix that is upside down from any matrix that has ever been built in any organization—other than the intelligence community, which was created in exactly the same Act, at exactly the same time, with exactly the same problem. The director of central intelligence has no money.

It is now fifty-five years later, and the DOD has evolved as an institution, with all of these OSD people, Joint Staff people, and all the rest of them who are working hard to make the peanut butter and jelly come out right. As you say, it's an enormous cost. The only entity that we do better than is the intelligence community, because there, as opposed to the secretary staying the secretary, the logical equivalent would be that he wanted to be secretary of defense and secretary of the Air Force at the same time. We never built up this enormously complex and costly set of systems to make the peanut butter and jelly come out right. The DCI is therefore a lot weaker than the secretary of defense is, but he still insists on being the head of the CIA at the same time. It's a very interesting issue.

There are solutions. First, there's the DCI's, which Tony knows more about than I do, but I don't think it's really effective. Second, there's the DOD's, which is a sort of chaos. Third, we could give the money to the combatant commanders and let them buy from the services. That thought process would be revolutionary, but it would be consistent with the Title 10 kinds of ideas that it's not the civilians doing it, but the military.

Oettinger: But imagine a warfighter being totally bogged down in the procurement process!

Stenbit: No, he doesn't have to procure it; he just gets the money to flow through his hands. My personal suggestion for all of this, which doesn't cost any money, is to insist that none of the service chiefs of staff retire from that job and that they have to become combatant commanders—but we won't tell them which service they'll command. I get to choose on the basis of what they did when they were service chiefs. That's cheap, but bureaucratically very tough, because you might have some accountability.

That's only a long way to say that I think it's a tough problem, and it's there forever.

Oettinger: Let me respond to all of you, because on the intelligence side the counterargument for the DCI also being the head of an agency is that if he weren't, no matter how much money he had, he would own nothing and would have zero leverage. So the argument goes back and forth. It's been going back and forth for fifty years.

Student: There's also sort of a competitive analysis motivation, or is that irrelevant?

Stenbit: That's the services. Mr. Rumsfeld's idea about how to fix this is to have the combatant commanders describe, top down, the capabilities they want and have the services compete to provide the capability in each engagement.

Student: That doesn't work for procurement, though.

Stenbit: Sure it does, because if they didn't procure the stuff that does long-range fires from wherever…

Student: That's a guess.

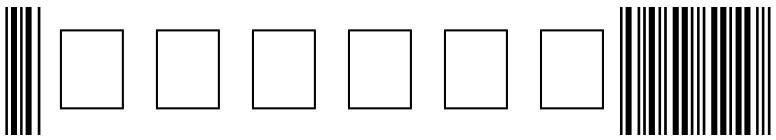
Stenbit: Oh, no, because today what happens is that they all get to come, they all get to share, and they suboptimize on the basis of "Everybody's got to play." But think of it in my world, where I have this network and I have value-added suppliers who tell me they're wonderful. I can check to see if anybody's ever not logged on. There are such issues that will come out of that kind of a top-down requirements process. If you're going to integrate horizontally—and that's really what we're talking about—you, as a ruthless buyer or user, must establish a criterion by which you measure if someone meets your requirements. You have to do that by good systems engineering and by understanding how to get the peanut butter and jelly to work. If one organization continuously does more of that, they're going to get more money. That's a very different rule from "Let's all get together and figure out what the lowest common denominator is." Remember, there's a lot of hope for JFCOM and for the Joint Chiefs, but both of them are in trouble, because they're both run by the JROC [Joint Requirements Oversight Council]. The JROC is made up of the vice chiefs of the services, and they will make sure that none of them loses, because it's a unanimous vote. It's a tough job.

Oettinger: On that note, let me thank you for a fantastic, informative, and stimulating session. We have a small token of our large appreciation.

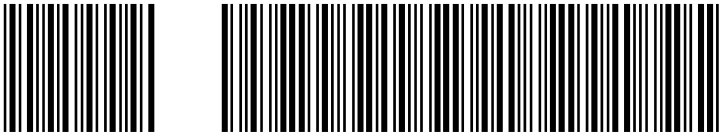
Stenbit: Thank you! Your attention has been great to let me babble on all this time, so I appreciate it.

Acronyms

ASD (C3I)	assistant secretary of defense for command, control, communications, and intelligence
ASD (I)	assistant secretary of defense for intelligence
ASD (T)	assistant secretary of defense for telecommunications
AWACS	Airborne Warning and Control System
C2	command and control
C3I	command, control, communications, and intelligence
CIA	Central Intelligence Agency
CONOPS	concept of operations
DCI	director of central intelligence
DHS	Department of Homeland Security
DOD	Department of Defense
GCCS	Global Command and Control System
GETS	Government Emergency Telecommunications Service
GPS	Global Positioning System
IA	information assurance
IPv	Internet Protocol version
JFCOM	Joint Forces Command
JROC	Joint Requirements Oversight Council
NCS	National Communications System
NIMA	National Imagery and Mapping Agency
NSA	National Security Agency
NSTAC	National Security Telecommunications Advisory Committee
OSD	Office of the Secretary of Defense
PPBS	planning, programming, and budgeting system
STU	secure telephone unit
TCP/IP	Transmission Control Protocol/Internet Protocol
TRI-TAC	Tri-Service Tactical Communications Program
TTIC	Terrorist Threat Integration Center
USAF	U.S. Air Force



Seminar2003



ISBN 1-879716-86-0