INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Information System Security
James J. Hearn

Guest Presentations, Spring 1992
Frank B. Horton; Roscoe M. Cougill; James J. Hearn; John M. McConnel; Richard L. Haver; Albert R. Lubarsky; Richard J. Kerr; Richard C. Macke

August 1994

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 1-879716-16-x **I-94-4**

Information System Security

James J. Hearn

Dr. Hearn has been the NSA Deputy Director for Information Systems Security since 1988. Previously, he was the Assistant Deputy Director for Research and Engineering (Systems Acquisition), the Chief of an Operations and Analysis Group in the Operations Directorate, and Chief of an NSA field station in Germany. From 1978 to 1982, he was Deputy Chief, then Chief of the Office of COMSEC Applications. From 1976 to 1978, he was detailed to the Intelligence Community Staff as Chief, SIGINT Assessment Division. Dr. Hearn began his career in 1964 as a design engineer with the COMSEC organization. He served as a project team leader and branch chief in COMSEC and as a division chief in various offices of the Operations and Analysis Group. Prior to beginning his civilian career with NSA, he was a naval officer assigned to the Naval Nuclear Propulsion Headquarters Engineering Staff. His undergraduate and graduate degrees are in electrical engineering.

Oettinger: I would like to introduce Jim Hearn, who is Deputy Director of Information Systems Security in the National Security Agency (NSA). You've all seen his biography. I would add to it only that I consider him a friend, and so it's a double pleasure to have him here with us today.

Hearn: It's a delight for me to be here and meet with you. I had the pleasure of meeting with some of you at lunch and know a couple of you. For instance, I know the gentleman in the background there from my job, working with him on various important topics.* What I want to do today is introduce you to my organization. Two predecessors from the National Security Agency have spoken in this program. In 1980, Raymond Tate** spoke. He wasn't in the job I now have. He had passed on to other things, but he came up here and talked then. And Harry Daniels,*** I think, was up here and spoke in 1986, and both of them spoke on something related to C^3 and telecommunications, or C^3 and how you fight wars, or something like that.

I'm going to have a more focused view than that, and what I probably intend to give you is a sense of my organization, which occupies a narrow part of the U.S. government but which, nevertheless, gets to see from that narrow perch a lot of the sweep and change of things that are occurring in the world today. I want to give you a sense of an asset that exists in the U.S. government, which I think is very valuable, and one that I feel is my major responsibility to keep, to make less fragile than it currently is, and to be frugal in its use. I have several vugraphs that I'm going to use to assist me, and I presume these will help.

I operate in a somewhat military style — I've been a civilian with the agency for 27 years, but it's run by military officers, so I've picked up some of the culture over that time, despite my sporadic attempts to reject it or avoid it, nevertheless, some of it stuck. I'll start with our mission, and the mission is something that sounds like a total quality management inspired (if I can use those two terms together) statement, but we're in the midst of some of that these days by direction and directive. Our objective is to provide leadership, to provide products, and to provide services. The emphasis here is on customers. My agency has had a history for many years of treating its work as something worth doing for its

*Dr. Barry M. Horowitz, President and Chief Executive Officer, The MITRE Corporation.

**Raymond Tate, formerly Deputy Assistant Secretary of the Navy and Deputy Director of the NSA.

***Harold Daniels, formerly Deputy Director for Information Security at the NSA and Assistant Deputy Director for Communications Security.

own sake, without too much regard for who was going to use it. We have slowly come to learn over the years that that is sort of a dead end if you pursue that too long. So the emphasis is on customers, and it's a secret customer set. It needs to protect classified and sensitive information — systems within our national security context. Now this is an unclassified statement (figure 1), for obvious reasons, and there are some phrases in here that blur what the classified version of this would say, but let's just try to describe that. There are a lot of pressures. If left completely boundless, it would be relatively simple to produce extremely good cryptography and information security to satisfy the nation's governmental and, I think, private sector needs. I mean, there would be a lot of implementation difficulties, but I think it would be a much simpler task than it is currently, where you have a lot of stakeholders, to use a phrase that's familiar to all of you. It was probably invented here. But there are a lot of stakeholders who don't want us to work quite as well or quite as rapidly as we can, and so within the national security complex, there are forces, contentions, pressures that exist in executing my mission. But that's our mission: to secure national security information systems.

Now our home is the National Security Agency, and there are two missions there: signals intelligence, which is by far the larger of the two, and I run the Information Systems Security Organization. There are three major themes to that organization (figure 2). There is what we call COMSEC, or communications security. The central feature there is cryptographic design. We encrypt information and give our users the ability to encrypt it and decrypt it, and to make it so good that nobody else can decrypt it, ever. Then there is computer security — I'll talk a little bit about the evolution of that. I'll also discuss why the forces of technology drove us in the late 1970s, early 1980s to widen our embrace to include this particular discipline.

The Information Systems Security Organization (ISSO) provides leadership, products, and services to customers that need to protect classified and sensitive information systems within the total national security context.

Figure 1

Our Mission

Signals Intelligence

Information systems security (INFOSEC)

- communications security (COMSEC)
- computer security (COMPUSEC)
- TEMPEST

Figure 2

National Security Agency (NSA)

There is something called TEMPEST, which is kind of on the wane now, but really can be characterized as a discipline that arose because in the early days when you had communications devices that consumed lots of power, even though you protected the information, it might leak radiation in a plain text sense, so that people with sensitive enough equipment could copy it and thereby bypass the protective measures you built into it. With the advent and advance of microelectronics and lower and lower power-driven devices, technology has solved this particular problem for us to a large degree, so it's something that is on the wane right now. So the technical disciplines, the pillars of our mission, are in the mathematics of algorithm design, the radio and communications science needed to implement them, and the computer science associated with the notion of computer security. Yes?

Student: Since you're talking about the last one, TEMPEST, is it some kind of electronic device?

Hearn: It's a phenomenon and it's radiation. It's information in electromagnetic form. The device emits signals, and if you don't attenuate them to prevent the emission, then you can subvert the protection measures you built into the device. So it's a phenomenon, and it's basically electromagnetic radiation and the conduction of electrical energy that it describes. Does that answer your question?

I understand from reading transcripts of some of the previous classes that the questions can come throughout, and that's fine with me.

Oettinger: Yes, well, you're about to move on to the next one. I've been harboring one, so long as you're willing to be interrupted. Are you going to

say more about the relationship among these disciplines, particularly communications security and computer security, in an era where what's computers and what's communications gets increasingly blurred? What are the arguments for and against treating those separately or as one seamless web?

Hearn: I'm going to try to do that.

Oettinger: You'll deal with that later?

Hearn: Yes. In 1980, or thereabouts, as I mentioned, when we embraced COMPUSEC (computer security), it was a separate discipline. It was a deliberate and political decision, and George Jelen's* paper, which he wrote from his 1982-1983 experience, "Information Security: An Elusive Goal," treated it very well. It described at some length the origin, the genesis, of this particular mission and the political basis for it. It was kept separate from COMSEC deliberately, but since then we have merged them.

I'll go into the evolution next. We'll start our history in the late 1950s, early 1960s (figure 3). I come from a very technical agency. We have always had a program to hire the best mathematicians in the U.S. whom we could get to come to work for the government. We offer them extremely challenging work on what we call the frontiers of mathematics. We have had some great success during many of the years that I've been with the agency in hiring tremendously outstanding mathematical minds to help design the mathematics that protect U.S. sensitive and national security information. We knew and recognized early on that just to invent the mathematics wasn't sufficient. Product people had to be able to implement our algorithms into various electronic devices, whether they were hand-held radios, a telephone on someone's desk, part of an Army mobile communications unit running around in the field, or equipment on board a ship, so that they could get sensitive information sent by shore naval facility, airplanes, and nuclear command and control.

All of these were applications of cryptography and secure communications, and to go along with the mathematics ability, the NSA, after its founding in 1952, began to hire very capable engineers to implement the mathematics into hardware. The agency had a very comfortable, somewhat informal, but very creative relationship with industry back in these years, in the late 1950s, until about 1970.

*George F. Jelen, "Information Security: An Elusive Goal," Program on Information Resources Policy, P-85-8, Harvard University, Cambridge, MA, June 1985.

Late 1950s – Mid 1960s

- Switching transistors for NSA-developed modules; >80 million, large user of discrete technology
  - 1962: first all-transistor crypto fielded

Mid 1960s – 1970

- NSA developed integrated circuits (ICs); >17% of industry IC output
  - 1967: Willis Ware/DSB report on vulnerabilities of computer systems
  - 1968: first crypto with ICs fielded
  - 1970: first KG on a chip

Figure 3

INFOSEC Technology Evolution – 1

There weren't so many rules in place then about competition in contracting, and how to award contracts, and all those sorts of things. And there was, in particular, a very talented director of research. His name was Mitford Mathews. He died before he was 50, I think, on a temporary duty assignment. He was a workaholic, worked 18 hours a day, knew as much technically about what was going on as did most of his people, was a great mentor, a great developer of people, and an inspiration. A lot of the technical excellence, in the engineering sense, that the agency was gifted with at this time was as a result of this man. But he had great vision to go along with technology; maybe that's part of genius. He saw discrete transistors as something that could make a cryptographic device useful to people in the field. We could make it small so a person could carry it around. We could put it in a jeep or in a tank; it didn't have to sit in a shore-based COM station.

In those days, the U.S. government worked differently. You could go down to the Pentagon and say, "Gee, I have a nifty idea. I think transistor technology would be great for building secure devices, and I'd like to have about $40 million to salt around to three or four companies to see what they could do with that," and the Pentagon would say, "Sure, that sounds good to me. Go ahead." So NSA had a lot of firsts. We were the first to field an all-transistor crypto device.

In the mid 1960s to 1970, we got into the integrated circuit (IC) game. We had at one point in that time period almost 20 percent of the industry IC output. That gave us tremendous leverage. We had tremendous buying power. We could have great cooperative ventures with industry in terms of what kind of ICs we needed to do our thing. That was a very effective motivator and gave leverage to our business. At about this timeframe, the first inkling of a new challenge came up, and Willis Ware, who is still at RAND, was involved in lots of things. He wrote a report that talked about the vulnerabilities of computer systems and, of course, in those days and through much of the 1970s, we were talking about stand-alone computer systems. They were known as automated information systems. I guess the word "seminal" can be overused, but I think that it could characterize Ware's report. It raised an alarm, but not many people paid attention to it. The U.S. Air Force did, and sent some teams around to look at various Air Force computer systems, and lo and behold, they found out that a lot of what Willis Ware was reporting on, was raising an alarm about, was true. There were a lot of vulnerabilities in operating systems.

In 1968, the first crypto with integrated circuits was fielded. This was in the Vietnam era. This was a device that, although someone could carry it around and use it to transmit, had very poor voice quality and people wouldn't use it. So we had a great technical success, but a lousy operational experiment experience. Although we had a first, it was far from a success. And then we developed the first key generator (KG), which is kind of the heart of a crypto device on a chip. All this just says that NSA was very much in the forefront of the INFOSEC mission and in the forefront of technology. We had a mindset that was "invent and develop," and we attracted some very good people because we had that mindset.

But beginning in the late 1960s and early 1970s, we were faced with some realities that caused us to radically change our culture (figure 4). The birth of the calculator and digital watches meant that we no longer commanded 20 percent of the U.S. IC industry. We went to much less than 1 percent. So we had to pay for special design features, special components, reliability, and those kinds of things, and pay in large dollar amounts. We fielded a second-generation secure voice system only six years after the first. It was a big improvement. It's still being used — 180,000 of them are out there. It went through several successful improvements

Early 1970s – present

- Birth of electronic calculator, digital watches in early 1970s
- NSA uses LSI (large-scale integration), microprocessors in products but <<1% of industry output
  - 1974: second generation microelectronic secure voice system fielded
  - 1981: computer security center established at NSA
  - 1986: first fielding of STU-IIIs (Secure Telephone Unit–3rd generation)

Figure 4

INFOSEC Technology Evolution – 2

since, but this was a major success story. There's another blip on the computer security screen, the fact that a computer security center was established at NSA in 1981, and then there's the Jelen report that I referenced earlier, which talks about this in some detail.

Then in 1986, there was the first fielding of a device called the STU-III. It's a secure telephone unit and it's relatively inexpensive — $2,000 compared to its predecessors, which were $10,000 and more. It was a great venture with industry, in that it would rely primarily on commercial parts and not necessarily parts selected especially for military use. During the Persian Gulf War, it was taken to the field and did extremely well in terms of operating reliably in an environmentally hostile environment — sand, heat, and that sort of thing.

But in this transition period here, the NSA folks went from being inventors on the edge of research, to people who were good at producing large volumes of things. We became a manufacturing organization primarily, instead of an inventing organization. It was a necessity. Our customers wanted things in large numbers that they could take out to the field to protect their communications, but it was a shift in our culture, and we lost something; in fact, we lost a great deal in terms of creativity and intellectual mass in our research area.

Oettinger: Before you go on, if I could just add a footnote to both of these figures (3 and 4), because

Jim has presented this from the point of view of his agency. I think it might be useful to comment that some of the trends ran more broadly. The early period, that inventive period, coincided with the nonexistence of an industry that was itself just being born, and if these things were going to be done someplace, there was no place to do it other than in the government or in a few selected laboratories. It was a period after World War II, when research and development were perhaps at their zenith in the U.S. There had been no period quite like it before and has certainly not been since, so the climate was right. The change coincided with the growth of an outside industry, so that the share had to decline simply because there was more growing. There was also a growing distrust of government, the Vietnam years, and legislation that made R&D in the government more mission oriented. There were a whole bunch of changes in the climate. So you're looking at some specific NSA phenomena, but also in the broader context, at coincident trends throughout R&D elsewhere in the government and in the larger community. Does that coincide with your observation?

Hearn: Yes, and I appreciate your helping me out of my little niche here to put it in the context that you just put it in. Yes, that's exactly right.

Student: I'm just curious. You're talking about things that are distributed widely, and you want at the same time for them to be secure. How are these gizmos set up, so that if your embassy catches fire and they take a STU-III, or if you lose one out in the desert and it falls into other hands, how can these things remain useful to American users?

Hearn: Well, the security of a crypto device is in the key or crypto variable, and not in the algorithm, the thing that does the actual scrambling and combining of the plain text to produce enciphered text. When you design these equipments, you basically assume you're going to lose some, and that you may lose some to an adversary who can reverse engineer the hardware. What you do in a simple sense — it's a little more complex than this — is when you lose one, you change the key, or you change the key periodically because you don't always know exactly when you lose one. So that shuts out the unauthorized user from the net.

Student: So it's not in the hardware, it's in the key that goes into it.

Hearn: Right.

Oettinger: One second ... I think it's fair to say that, at least from open historical sources, a lot of the breaks of crypto have been due to carelessness, as in changing keys, rather than in compromising of the equipment.

Hearn: Yes, rather than an inherent weakness in the hardware and the algorithm.

Oettinger: It's sloppiness; sooner or later somebody does something stupid.

Student: The most notable cases or a lot of the cases were neither of these, they involved someone posing as a friend who was in a position to get access.

Hearn: Well, yes. The trusted insider is the toughest problem of all to defend against, either in the computer security area or this area.

Student: I have a couple of questions. You talked about the increase in reliability. How much of that is due to satellite technologies?

Hearn: Well, let's see. Satellite technology was a driver to reduce the size of electronic gear, so I guess it was an agent to create more reliable things. I can't say that we borrowed directly from satellite technology in all cases. We certainly knew how to select parts so you would build devices with the best, and then in the combination you had the most reliable device. Satellite technology does that also. For obvious reasons, you can't get at satellites to fix them.

Student: If you stay away from HF (high frequency), for example, you would have a lot better quality when you're listening.

Hearn: But we've built HF crypto that can last 10,000 hours, on the average, before it has to be fixed, and so we kind of overdo it. We don't necessarily tie our contributions to the communications system or crypto to the reliability of the whole system. We build it as well as we can; at least, we did in the past. The STU-III, as I said, was a departure from that because it was made largely from commercial products because we had to get the thing built quickly and out there in large numbers. It's really a harbinger of things to come, where more and more we are going to be tied to commercial practices and the rhythms of industry's way of doing things, since we cannot have a stand-alone or separate pace for our business.

Student: As you go through the history, what does that do to your actual relationship with industry and with the academic world, in terms of your own security requirements? I can remember listening to Admiral Inman* in the late 1970s, talking about the openness of academics in the mathematics field and the security fields as being a very difficult thing to deal with, and his trying to hold that in and keep it for his own use here in the United States. Is that still a problem? Or has that problem gone away? It seems that your history would say that that might even be more of a problem than it was originally.

Hearn: Yes, it's more of a challenge certainly than it was. Inman was the first one to open the door, so to speak, and successive Directors (of the NSA) have opened it wider. I don't imagine pre-Inman that anybody from our organization would have come up here and given a talk, as I'm giving this afternoon. But I look upon it, and I mentioned this to Tony last week when he visited us, as something akin to survival. The way the world is, we have to be so much a part of it, not only with industry but also with congressional support and other things that we need to sustain life; in the sense of mission, we have to be more open. I mean, we just have to be very much better in our mission at sharing its usefulness and its importance, along with protecting those things that are really classified. I think in years past we were perhaps too conservative and overzealous and overprotective, but that doesn't mean we've hit the point where nothing needs to be protected, because we haven't.

Oettinger: In yesterday's mail, there was a sign of what you're talking about. I received an announcement from the Association for Computing Machinery (ACM) and other societies sponsoring a conference on computer freedom and privacy. One session is titled "Who Holds the Keys?" and it says that cryptography has become a battleground for personal privacy and national security. Should the government be permitted to restrict the use of cryptography or to restrict export of products that use cryptography, and what legal protection should exist for enciphered communications? So the issues Jim describes are today a subject of public debate at meetings sponsored by professional societies. That's a significant change in the climate.

McLaughlin: Well, I think the other thing is that we're seeing changes cut both ways. I suspect that there are some stellar mathematicians on the market today who would be happy to sign all sorts of nondisclosure agreements, or something. It works that way, too.

Hearn: I have a couple of examples from the environment part of this presentation, which explains why we're more open than we have been in the past; we're still trying to follow Inman's example in terms of being judicious about what we share and what we still feel we have to protect.

The next slide (figure 5) has a quotation, that I know several of you in the room are familiar with because I've had discussions with you about it. I'm not saying I endorse everything this publication says or anointing it with some sort of NSA holy water, but I think it's very useful for there to be some intelligent debate and discussion about the value of information, and about informed people's views about how indifferent or unconcerned vital segments of the U.S. information industry and information ownership are about the protection or the fragility of their information and protection that should be given to it. This publication gets into some of that. Also, Dan Knauf,* who was a member of this program, in 1988–1989 wrote a very fine paper that talked about the value of information and the whole spectrum of attitudes in the U.S. on the part of companies, and their concern or lack of it about protecting information. This sort of thing is one of the elements of the environment that we find ourselves in and it has raised the level of discussion about these sorts of activities.

I've got two or three vugraphs on the environment (figures 6 and 7). All of this is very well-known to you. On the one hand, the sharing and distribution and access to information are enriching, value-added experiences. On the other hand, as Tony just read from that ACM brochure, this mindset exists more and more, not only in governmental circles, but in private and academic circles. Information owners have some need to protect and restrict access, and to parcel out, as it were, clumps of information just to selected audiences, whether it's a company, a government, or between nations. We have many, many challenges in our path to do this. In many ways, the technology to do this is either in its infancy or doesn't exist, and one of the main

*Admiral Bobby R. Inman, former Deputy Director of Central Intelligence, Director of Naval Intelligence, and Director of NSA.

*Daniel J. Knauf, *The Family Jewels: Corporate Policy on the Protection of Information Resources*, P-91-5, Harvard University, Cambridge, MA, June 1991.

"The nation is on the threshold of achieving a powerful information infrastructure that promises many benefits. But without adequate safeguards, we risk intrusions into personal privacy (given the growing electronic storage of personnel information) and potential disasters that can cause economic or even human losses."

Computers at Risk, Safe Computing in the Information Age, National Research Council, 1991

Figure 5

Views of the National Research Council

functions I have is to rebuild a research enterprise at NSA that will, in cooperation with industry, be able to address this technological challenge and help to solve the problem better than we can solve it today. Yes?

Student: Dan Cougill* talked last week about virus problems in Desert Storm. That would seem to be a big aspect of computer security. Is that a problem that you're working on?

Hearn: Yes.

Student: Do you see that or treat that as a potential weapon?

Hearn: I don't, because my job is not to stop other people from communicating. My job is to protect U.S. communications, but certainly most things have two sides, and the virus certainly has been written about in the press recently. It is something that has the character of a weapon under certain circumstances. Yes?

Student: A flippant question: Can you confirm or lay to rest a *Newsweek* article on the virus in the Iraqi air defense network?

Hearn: I can't, because I don't have direct personal knowledge of the details.

Student: Going back to your point about industry, it seems like traditionally we've been focusing on securing embassy communications. I believe there are indications, for instance, that some of the European governments have been using their resources to tap into American industrial communications, such as fax messages. Do you see this as a problem that NSA or the government would try to combat?

Hearn: I will give a description in a few minutes of how the government is organized or disorganized to address that problem, and it has to do with the NSA/NIST (National Institute of Standards and Technology) relationship. But certainly in all the scenarios that are being developed at NSA and for the future of who will be our adversaries, who will be our allies, and what needs to be protected — economic, technological, financial information are items of concern. Are all the users, the people who own that information, sufficiently alerted to that? No. And so how does the government organize itself to help in that process? We're going to talk a little about that in a few minutes.

I have a cartoon here which is a little technical, but you're all such bright folks that it won't be any

- Interconnected desktop computers have become an integral part of the workplace.
- Unquenchable demand for information access.
- "Open Systems Interconnected" — new network technology allows building LANs, WANs, and Internet connections to provide unrestricted access and information flow.

BUT

- Ready information flow (which the networks are designed to provide) is the core of the network security problem.
- Technology to control access and limit information flow is in its infancy, or has not even been conceived yet.
- Network/Internet technology is very complex, interconnected network structures are even more so.

Figure 6

The Environment

*Brigadier General Roscoe M. Cougill, USAF, Director, C⁴ Directorate, Joint Chiefs of Staff.

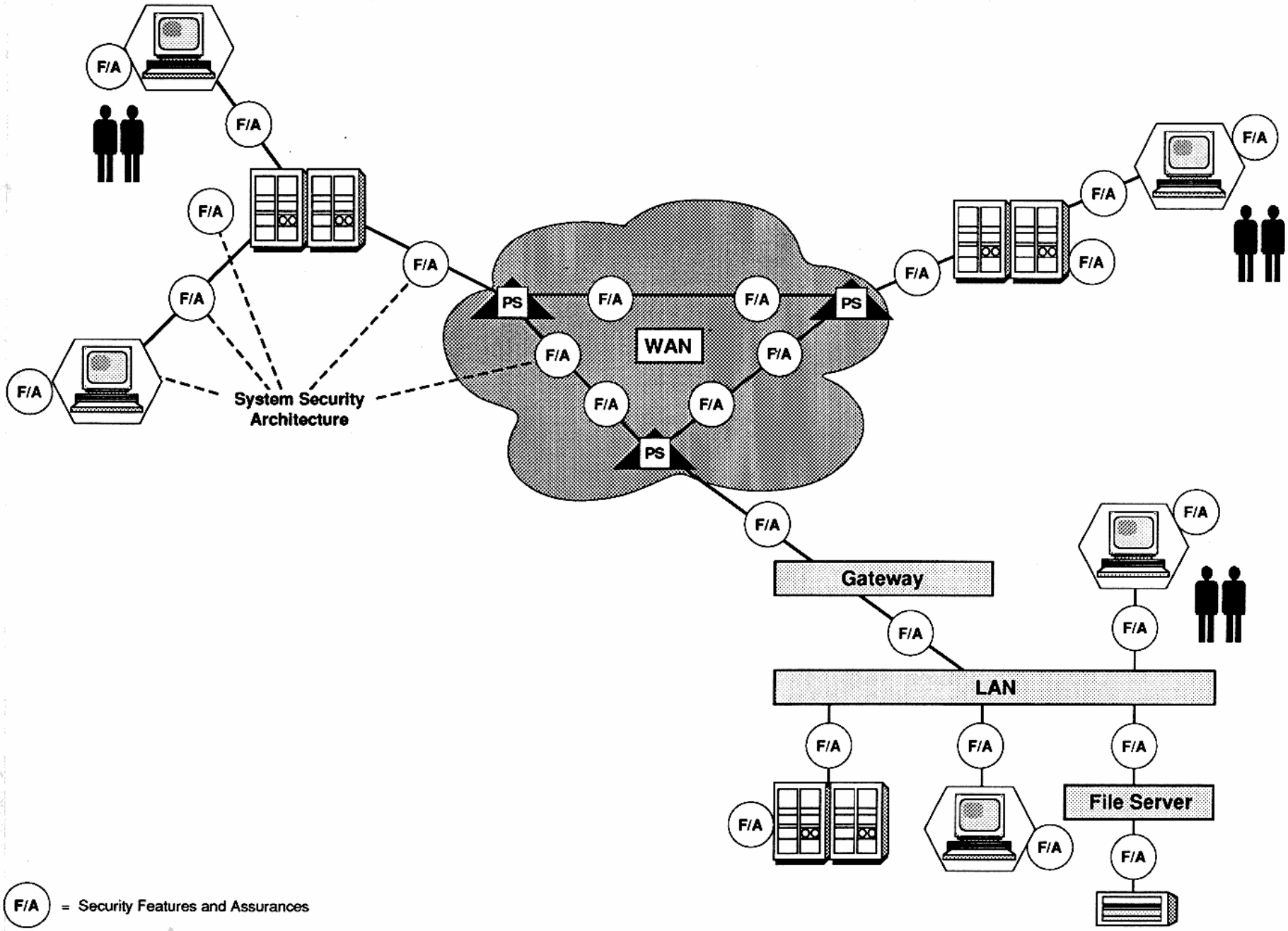

Figure 7

Security Services Provided by Features and Assurances at Multiple Places

problem for you (figure 7). It captures the old and describes the current environment just in a kind of network form for those of you who prefer pictures. Just ignore these packet switches for a minute. In the old days life was pretty simple. We had a communications station here and a communications station here. We were talking about data in transit, going from A to B, and we put a crypto here and a crypto here: encrypt-decrypt. These two people could communicate and all we had to do — in quotes — is make sure they had the same key, and they could protect those communications. Living back then as a young man, I'm amazed at how complicated I seemed to think all that was, given where I am now. But anyway, that's maturation, or experience, or something. I don't know what it is. But that was the main focus of NSA. When Willis Ware came along in 1968 and the Air Force teams were working in the 1970s, they were looking at a situation something like the upper right of the figure — but this would be an isolated computer center, not hooked to anything, just batch processing. You'd have people here, computers here, and the concern was, "Can I build this to create the environment for access control and authentication, so that an unauthorized person can't get data out of the machine?" That was the model for the stand-alone era of the 1970s.

What we have now, as you all recognize, is an environment like this. The F/A here means features and assurances. This is a little bit of getting into the noise of my existence but, bear with me. Features are things like: confidentiality — keeping the data away from an unauthorized person; authentication, which means making sure that you can relate the one who wants to use the data to his privileges to use that certain kind of data; auditing means making sure that you have security-relevant audits that you can check for unusual behavior, maybe to see if someone's using your system who shouldn't be. These are the kinds of features people now want in the network environment.

Assurance is where it gets in a very large sense into my business. Assurance is the amount of effort you put into making sure that all these things do what you think they're going to do, that there are no hidden flaws that will undo your design, and that you have built these devices so that they are safe from most reasonable postulated attacks. And that's expensive, because our history was that we would take five or six years to evaluate the hell out of something before we put it out in the field. So we were very highly confident that the device, the equipment, or the system, was relatively invulnerable. We don't have time to do that anymore. So, in addition to the challenge of dealing with an interconnection of things like this, we have less time to put the A into all these devices and all these products. We have to figure out how to do it smarter. This is just a wiring diagram to depict in picture form the environment that we are now working in.

Let's look at some of the other parameters of the environment (figure 8). Some of these people probably come up and speak to you from time to time. These (the office of the Assistant Secretary of Defense for C³I — ASDC³I) are the people in the Pentagon who oversee us, and they change over about every two or three years. Everyone comes in with his or her own political agenda. That's fine, that's life; you have to learn what their next aspiration is and how to deal with them, educate them in your business, and get them to the point where they moderately understand. Then, they're off and you have a whole new set coming in. The current theme — well, it's been around for a while — is multilevel security. This is the savior, this is the panacea. If we have these kinds of devices to automatically protect and sift and route information to the right people at the right time, with the right credentials, then we'll be able to save a lot of money. On that previous chart (figure 7), instead of having a particular constituency using one part of the system and another constituency using a second part of the system, everybody will be able to use the same system. Technology will sort out what data should go to people authorized to receive it. Then there is an overseeing organization headed by a guy named Paul Strassmann,* who is the Defense Information czar. I don't know why these people always get called czars, but he's the czar. They come in and say, "Well, we're going to have this corporate information management system. What used to be the Defense Communications Agency and is now the Defense Information Systems Agency (DISA) will be in charge of it and the goal here is to reduce the number of the communications systems that are out there, to have different kinds of people using the same systems, and things will be done more cheaply with greater efficiency." A lot of that sounds reasonable, but the timing and the technical underpinnings that allow you to do that are critical here. There are a lot of components to the DISA mission involved in achieving this sort of consolidation of communications and information resources.

*Paul A. Strassmann, then Deputy Assistant Secretary of Defense (C³I).

ASD (C^3I)	Promoting system integration; theme: multilevel security = $$$ savings The new corporate information czar
DISA	The Defense Information Systems Agency New role in DOD information systems ▪ ADP acquisition ▪ Networks ▪ Protocols and standards ▪ System security architecture (DISSP)
The Services and Defense Agencies	Want networking, but don't want DISA (or anybody else) in control of their networks Are slow to be weaned from independent network security initiatives

Figure 8

Players – 1

Oettinger: Just a footnote on the mention of Paul Strassmann, if any of you are interested in pursuing that further: Paul has written several books on the subject. The metaphor that comes to mind unfelicitously is *Mein Kampf*, but I don't mean it quite that way. But you can read what is in the back of his mind in things that you can look up in the Widener Library. There are at least two or three books that he wrote before taking on this job.

McLaughlin: They aren't recommended unless you really work in that field.

Oettinger: Yes, that's a good point.

Hearn: I'm doing all this because of the environment, and all these things are part of the environment, including technical challenges, personality challenges, and axe-to-grind challenges. We have an organization that's in some ways been in the backwater on a lot of things, and now has had thrust upon it several new major missions that we're expected to perform immediately. And you have the cultural clashes that run through all of this, as they do in all things in life, with the services, especially in these days of resources reduction. Remember, the leaders now have grown up with a stand-alone — stovepipe, I guess is the phrase — era and they're saying, "You want us to combine all our assets into one communications and information services pool? Say that again?" And they're greeting this with some degree of skepticism, to put it mildly.

Student: Since you're going through the players here, do you see any major changes here for you in the tug and pull of resources, as well as with the czar dynasties?

Hearn: Well, the Boren-McCurdy* and other proposals are focused mostly on the intelligence community, which is a customer of ours for security devices and leadership and services. What changes occur there will ripple into my domain, but nothing that they have come out with explicitly deals with radical changes in communications. Congress hasn't explicitly addressed major initiatives that would upset my mission, except in the fact that my customers may be radically altered, so therefore my relationship with them will be altered.

Oettinger: Or, if I may put it another way and see if you agree, what is described in the top three lines — the $ASDC^3I$ — the incumbent and his organization are relatively new and reflect both this adminis-

*Senator David Boren (D-OK) and Rep. Dave McCurdy (D-OK).

tration and the current Congress' view, so in a sense, that's in advance of what's happening in the rest of the community. It's already had at least one wave of reorganization, unlike the others. Is that reasonable?

Hearn: Yes, Duane Andrews is the ASDC³I. He reports to Secretary of Defense Dick Cheney and he's been in the job now two, almost two-and-a-half years. It's really in some ways an effete job because he can't hire or fire all that much, so it's taken him a long time to build up his staff.

Student: I guess what I was thinking of, sir, was the fact that the bills would pull the "I" out of that C³, essentially, and that would mean that your customer is separated now from what you deal with on a day-to-day basis, in terms of communication and security. Will that affect how you do business? Is it better to have them combined, or is it better to separate them and make them two different organizations — two unique organizations is what they'll become — two czars, two fight leaders.

Hearn: It's not going to have a major effect because our mainline customer has been the military, whose systems include intelligence information but which exist for reasons other than just passing pure intelligence information. They have been more than a challenging customer.

Oettinger: And besides, the notion of the C³ and the "I" in that box is a fairly recent phenomenon, which hasn't made much difference from the previous strategy.

Hearn: Maybe this will chip away at answering your question (figure 9). The intelligence community is separate, whether it's reconstituted from the way it is now, or whether the CIA's influence is diminished or the Department of Defense's influence is diminished. Whether you do away with this acquisition component or that, there is still going to be an intelligence community. And they have always been separate from a lot of our other customers — the ones from the previous page (figure 8). They have had their own systems, mostly fixed plant, but some tactical, and they look with a degree of horror that's somewhat understandable at being connected to the same pipes that carry logistics information, personnel information, and those kinds of things. So they want to remain aloof. Now, if the powers that be, whether it's Congress, C³I, or whoever, force a migration of major components of intelligence information into logistics systems

The Intelligence Community	Ultimate citadel of "system high" Major concerns with integration
NIST	Primary government interface to industry and standards groups (ISO/ANSI/IEEE, etc.) Expanded role in network security via PL 100–235 (Computer Security Act of 1987)
GSA	Using FTS-2000 as springboard to launch into role as comprehensive provider of networking (WAN) and security services—the "integrated federal telecommunications system"
Industry	Playing dominant role in defining network security standards and protocols Confused about government roles and intentions in network security

Figure 9

Players – 2

information, personnel information, this becomes a massive challenge to manage.

Student: Isn't that going to happen on systems like Copernicus, which is the Navy system to do that very thing — to move information around?

Hearn: That's Admiral Jerry Tuttle's objective. As various forces push this community into sharing common information services, then there are potential security problems, and the ante is really raised.

Oettinger: I can't resist a personal anecdote at that point because organization charts are one thing, but reality is another. I'm thinking of a problem that we were trying to resolve over sharing of data resources among a couple of intelligence agencies, and three years were spent on delaying that, by virtue of an argument over how many columns each would put in an 80-column card devoted to which piece of information. You know, 35 years later, the details have changed but the bureaucratic infighting on what's mine and what's yours continues. So what happens in the Congress and what happens in the field are still years apart. There's a lot of room for maneuvering.

Hearn: Public Law 100-235, otherwise known as the Computer Security Act of 1987, split the responsibility for the protection of federal government information between NSA and the NIST (figure 10). NIST has the responsibility for something that's called "Sensitive but Unclassified," and NSA has the rest of the stuff, which is national security, mostly classified. Having two government agencies, which are really very asymmetric in resources responsible for information protection, has complicated life for us significantly. But we have to work on standards jointly now, of various kinds. We have very different relationships with industry. We have very different appreciations for the value of information and it's a fascinating thing to have experienced in my career. I think we have a pretty good working relationship with the NIST now, but the relationship is something that Congress created. Their real intent — I won't say everybody in Congress, but some of them — was to put NSA out of the picture for anything but intelligence and defense community orientation. What Congress did not realize is that the techniques, the products, the approaches, to protect the information — think back to that features business, the F and the A that I talked about earlier — are basically the same, whether you're talking about classified or unclassified sensitive information. The big difference, at first approximation, is in the A, the assurance. For the unclassified sensitive information, you have to take fewer pains, worry a lot less about its exploitability, so that's the difference and Congress failed to appreciate that. NSA and NIST have to remain locked together to address a lot of the nation's questions and needs in the area of security.

Oettinger: May I take issue with you on that because, you know, part of the problem is that some of it depends on what your mission is, and what you're looking at. Some of that is sensitive stuff in an era where there's concern over economic things that are not necessarily classified in the legal and directive sense of the word. The assurances for these things may need to be just as high, and it's in the eyes of the beholder, in part. It's simply a different regime of dealing with this, and it's only partly congressional whim. It's part of a problem in a society like the one you guys are dealing with: changing concerns under a fairly fixed legal regime. Or am I off the wall?

Hearn: I'm somewhat a victim of my experiences. If it's not nuclear secrets, or something like that, then I'm still learning to connect other kinds of information as requiring a big A, instead of a little A. It's sort of assurance. I accept that. That gets into the whole area, at least in my view it does, of classification. Perhaps a radical revamping of that whole classification system in this era of change ought to be looked at now.

Enforced NIST's COMPUSEC role for unclassified information

Requires federal government agencies to protect sensitive* information in government computer systems

*Sensitive: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest...or the privacy to which individuals are entitled...."

Figure 10

Public Law 100–235 (Computer Security Act of 1987)

Oettinger: Well, that and something else, which is implied. There is always the question of what protecting U.S. assets means? What is a U.S. entity? What is a U.S. person in an era where most corporate entities are in many different ways multinational? It seems to me that the problem has gotten vastly more complicated and continues to get more complicated day by day. But your question, to my mind, doesn't have a simple answer. It's open.

McLaughlin: Tony, it strikes me that the Congress is pressed with reinventing these vulnerabilities. I'm not saying that there aren't real vulnerabilities but, you know, a trillion dollars a day or whatever passes through New York City electronically. It's not like there's nothing being done out there by private firms to protect stuff. And the media and Congress every once in a while sort of decide that this is a new problem, and we have to launch a great initiative to correct it. I think that what they have found now in part is the fact that there are an awful lot of people making market decisions on whether this stuff is worth protecting, and what the price is of protecting it, versus the value of what they might lose.

Hearn: Yes, but again, the classification of the whole thing has to be evaluated.

But, getting back to the charts (figure 9), I mentioned GSA just for completeness. They have no money and they're in charge mainly of the civil parts of government. They pretty much have to live off what we invent or just develop some standards for it. But they certainly come to us for solutions. The role of Industry can't be emphasized enough in my view. Our dependence on industry in this country is critical for my mission. The U.S. still has a somewhat robust information technology industry, and without that we would be dead in the water. I get first-hand insight into that when I visit my colleagues in some of the Western European countries — the U.K. and Germany, to name a couple, who have either vanishingly small or nonexistent information technology industries, in the sense of having major PC manufacturers. They do develop wide varieties of operating systems. They just don't have much in the way of an industry, and my counterparts in those countries are really weakened considerably as a result of that lack of a robust, indigenous information technology industry. The extent to which I can do my mission is very dependent on the continued robustness and strength of the U.S. information technology industry. Yes?

Student: I'm not exactly sure what NIST is. But doesn't industry also play a part? Industry plays a role in making the standards, as much as the equipment or hardware.

Hearn: Your question is "What's NIST's involvement in the standards part of it?"

Student: I'm not sure what NIST is, I guess.

Hearn: NIST used to be the National Bureau of Standards. Three or so years ago, they became the National Institute of Standards and Technology.

Student: So, industry is developing the standards?

Hearn: And government. In Europe, the government is chartered, among other things, to manage and develop standards for all sorts of things. But in the U.S., I claim that industry has a very powerful voice in doing this. I mean, there was a time, according to some senior NIST people whom I've come to work with, that if a big manufacturer did not want a certain thing to become a standard, they would just say, "This isn't becoming a standard in the computer industry." They were that powerful and NIST could not override that. That's not quite the case in European countries, where the government is very powerful in the standards world. NIST is a legitimate governmental arm through which the standards process is affected in the U.S., but there are a lot of players, a lot of stakeholders involved in that.

Student: In my opinion, it seems like the industry has a large stake in these standards for their own benefit.

Student: I think that cuts both ways. I think that as long as there is an equal benefit or disbenefit, the standards work. But if there's an entrepreneur who has an advantage, then that has entrepreneurial value, and none of those standards will mean a thing. They'll sell a product and have the advantage. So because now everybody is dealing with this standard thing, there's no market and no entrepreneurial idea that's complete, but I believe if one were to emerge, this would all be kaput. If one doesn't, then this will have meaning. So it will really depend on whether there's sort of a spike, or whether it's sort of a gradual evolution product that we're talking about.

Student: A little confusion in my mind. You said, if I understood you correctly, that the dependence of your organization on industry is critical. At the same time, people in Germany, who have the same creed, are weakened by nonparticipation with industry. So who is better off? Who is in an advantageous position?

Hearn: I can give you an example. I mentioned a device called the STU-III, secure telephone unit three. Since 1986, we produced about 225,000 of them. They're used mostly by senior U.S. government officials, the military and intelligence communities, department heads, and a lot of troops. It costs $2,000 for that device, as I mentioned. The German equivalent, not nearly so sophisticated, costs $30,000, is produced only in the hundreds, and it took 10 years for the Germans to produce that device. That's an example of the power that AT&T, Motorola, and GE bring to solving that kind of problem in the U.S. sense. They would compete, each build a product, and compete with each other on a price basis. As a result, the customer, the U.S. government, got a very fine product at a fairly low price, compared to what other countries get when they go to an industry that's government-supported. Maybe that's what makes our information technology industry so robust, compared to a lot of other countries I could name. If we could do something like that in commercial electronics, then maybe we could buy an RCA Walkman, or something like that. We haven't been able to do that or recover that market.

I haven't answered your question, Tony, about the organization. If you refer back to the wiring diagram (figure 7), you can see the way information is now passed. You have to look at the network as a whole from the disciplines of computer science, engineering, and mathematics to figure out how to distribute security solutions and where, for a given architecture, the optimum solution set is. So we have combined those disciplines in my organization, and we have a multidisciplinary approach to looking at the security problem.

I have two vugraphs (figures 11 and 12) to finish up with, at least in this part of the discussion. A lot of this I've touched on already. Clearly, we've gone from a product orientation to a system orientation, with all the complexities inherent in that transition. We used to have very stable architectures. The military would have a system that was uniquely its own, built from the ground up. It would be in place 10, 20, 30 years. Now, we have a very dynamic architecture. We have the war scenarios of the future: future Desert Storms where we have to help the U.S. talk to itself and to a variety of coalition partners in whatever part of the world we find ourselves. We have to have an architecture that embraces that sort of thing. And we don't have the time to get ready to do that, in terms of four or five or six years. We have to be able to be very flexible in achieving this sort of state. The focus used to be on protecting the information from exploitation, and to some degree on authentication, knowing that the person receiving it or sending it is the person for whom it's intended, or the right sender. Now we have a variety of security features that people want in their information systems. And availability is a major one — that's the virus business that the gentlemen asked about, and whether that could be used as a weapon — the Internet worm that took down a fairly significant system for some period of time. One thing the military cannot stand is a lack of availability. Can we come up with devices, techniques, procedures, policies that will enhance or ensure the availability of the communications system, so it will be there for the user when he wants it?

We've gone from the physically isolated system to a distributed information system, and people want multilevel security in the context that I used just a short while ago. They want to be able to put a whole range of data, from Unclassified to Top Secret, in the same pipe, handled by the same devices, and have technology sort out that certain kinds of data go only to the privileged or legitimate user. And we've gone from a world where NSA could take five, six, seven years to build a product with government-furnished equipment in the COMSEC world, to a commercial-off-the-shelf environment where we need to partner with industry so that they build security features into their equipment and operating systems, and we in government can put some money into the development of some of these, so that industry will see that it's within their risk framework to take our development and to produce it in larger quantities for customers. Yes?

Student: Is there any trend for trying to do these things at lower costs these days?

Hearn: It's an imperative. I mean, theoretically it always was, but in these days of reduced resources, it's certainly a tremendous driver. The STU-III, again, at $2,000 is exorbitant, but it's all relative, depending on where you are. Compared to a $10,000 STU-II or a $30,000 German device, it's in the right direction. The next thing would be to have a $1,000 one. So, the pressure of cost is certainly always there and will be even more so from now on.

We could be much more deliberate and make sure that we put out something that we had exhaustively evaluated and knew was as free from vulnerabilities as humanly possible (figure 12). We're now accelerating equipment development: The pace of technol-

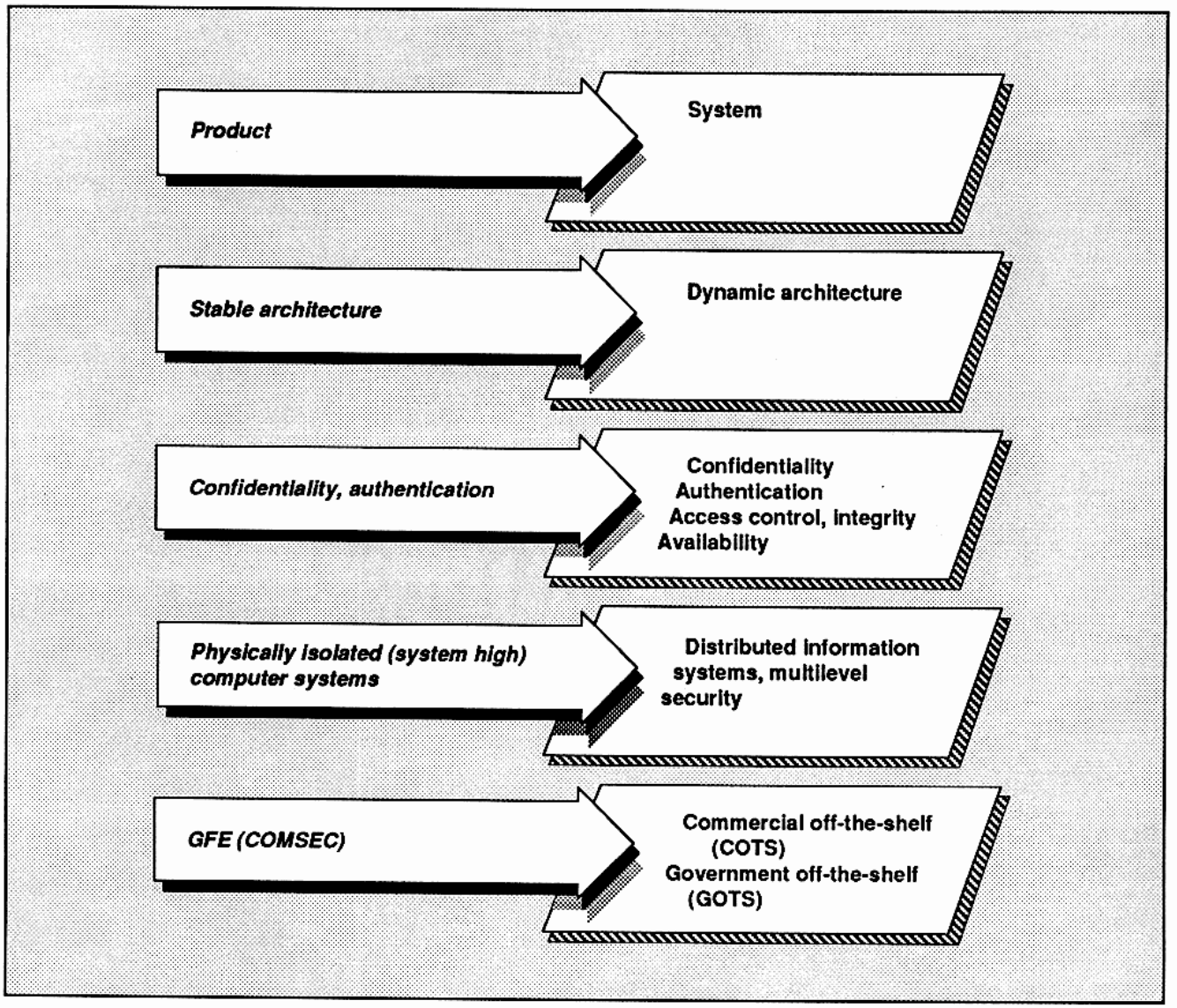

Figure 11
Trend Lines – 1

ogy rollover is every 15 months to two years, depending on whom you speak with, and that's the kind of rhythm we have to adapt to. There were relatively few product types in the past; now, we have hundreds of product types to deal with. The *IEEE Spectrum* of seven or eight months ago had a list of workstations. It was four pages long, and there were 11 or 12 workstations per page, so we had 45 different U.S. and a few foreign manufacturers of workstations. That's our target environment now. We have to target our security solution for the hundreds of product types, not just a few of them.

Another complication — we used to have a known adversary, we could focus on the Soviet Union. That was the threat. Now we have a much different threat, and what we're transitioning to, I don't know. There are probably some people at Harvard who can tell us what we're transitioning to, but they probably wouldn't be right, either. We're going to coalition warfare — come as you are — whatever you have, that's what you're going to fight with and that's what you're going to communicate with. We've had a period of stable funding but that also is changing.

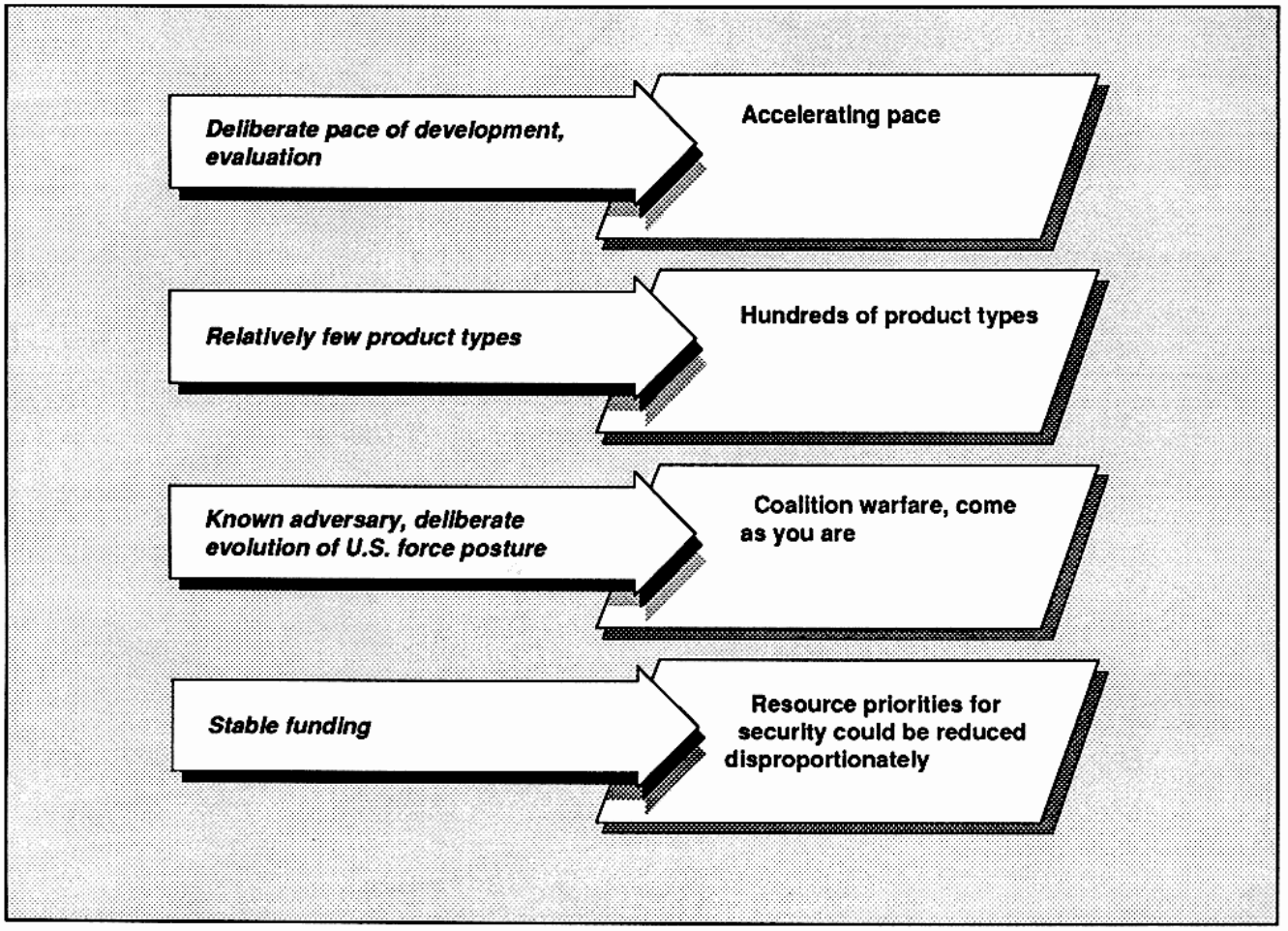

Figure 12
Trend Lines – 2

We've worked very hard with the military, and I see a modest improvement in my 25 years of working with them in their consciousness about needing security. It was interesting to read the 1989 presentation of John Myers* , who was then director of DCA. One student asked him, "Gee, you've just said some neat things about DCA and systems, but you never mentioned security." John Myers was a signal officer for 28 years, and that yields an interesting phrase. He said, "Well, I didn't mean to 'disinclude' it." I had never heard that word. And I said, "Does that mean that he did, or does that mean that he didn't?" But it really captured nicely the challenge that my organization has, again in a cultural sense, of keeping the need for security in the minds of these people who are primary users. They're the people who provide the money for us to do our thing, and yet that continues to be a challenging task.

Oettinger: I had a couple of thoughts that derived from what you said about this chart, because you were talking earlier about focusing on customers. You've just mentioned the military and how hard it is to keep them focused on security, and so on. Now, let's go back to what you also said about NIST and other customers, and John McLaughlin's remarks about Congress every once in a while getting on their high horse. When you're going

*Lieutenant General John T. Myers, "Future Directions for Defense Communications," *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1989*. Program on Information Resources Policy, Harvard University, Cambridge, MA, 1990.

against hundreds of product types here that have to be protected, it seems to me that the problem that protection is facing is that the number of types erodes the base and the amount of resources available to protect each product type, unless you get smart, or lucky, or both, and get very generic. If you have the military, as you say, hard to convince that this is something worth doing, then you have a difficult sell to your primary customers. If the assurance of sensitive stuff is, except for an occasional congressional up-in-arms, a ho-hum kind of thing, then there isn't a hell of a lot of incentive for manufacturers to produce something for an "iffy" private sector sensitive or nonsensitive market, or a fragmented military market that doesn't necessarily believe in the product. That sounds more pessimistic than what you characterize. How accurate is that as a picture of what you're facing?

Hearn: Well, there was a time in the mid-1980s when one of my predecessors really believed that the need for security in the private sector would burgeon and become so great that industry would respond, and so the government wouldn't have to invest to do that sort of thing. That turned out not to be the case. Fortunately, we have a sufficient level of awareness in the military now, Tony — the [Duane] Andrews, [Jerry] Tuttles, people like that, support our mission. We frequently have to go and remind them about it, but they're always responsive when we remind them, which is a hell of an improvement compared to 20 years ago.

Now what happens when the resource atmosphere gets a lot more grim is something else. We may run into a situation that you described, when people say, "Well, I'd like it, but I can't afford it." But that's the challenge we have. Some of us think that, "Well, maybe there'll be a Pearl Harbor in terms of an information loss catastrophe before we get a stable funding environment here." When I visited Sun Microsystems a few weeks ago, Scott McNealy, CEO of Sun, came by to talk to us, and he called it a "fire in the lake" syndrome. He lived near Lake Erie and talked about the time when it spontaneously caught on fire. That had to happen before people would clean it up. So he was saying that people's attention would be captured only when something like that happens. It's not a certainty, but I think we have to look at some of the worst-case scenarios and try to work against them.

McLaughlin: Let me suggest a trend here. It seems to me that part of this is like the special requirements for military computers 10 years ago, where everything had to be hardened and painted green, and we had TEMPEST and whatever. Today, with low power emitters and the commercial dynamics of protecting laptops from being dropped, it's almost a non-issue; commercial-off-the-shelf stuff can provide all those features cheaply. I have a suspicion, especially with cellular telephony or wireless telephony, that if you start talking about millions of digital units being produced in four years out or something, the economics of providing security in a mass market becomes much more attractive. And I think an awful lot of the industry level is price-sensitive. If you can provide something relatively robust at a relatively low cost, you'll sell a lot.

Oettinger: It's not clear, though, that that will manifest itself. I mean, what you say on board an airplane and what you say if you walk in the middle of the park on down the street may be quite different, because you know that the guys in front of you, in back of you, and at the side of you in an airplane could overhear your conversation. It may be that folks, when faced with the question of spending money for securing a cellular telephone, will just treat the cellular telephone as if it were talking on an airplane and not bother. It's not clear. The history of these markets materializing is rather poor.

McLaughlin: It's so far from a bargain, $2,000 for a telephone. Why, I can buy a decent instrument for $25, you know, or $30!

Hearn: There's a real recognition of the power of distributed processing now in a lot of companies, where PCs that have so many thousands of millions of instructions per second (MIPS) are just sitting there, not being used. It gets at some of the networking security issues as to how you use it. I think some industries are really looking at trying to figure out ways to do that. It's a lot cheaper than a supercomputer but security issues are a more difficult aspect of distributed computing.

I take John's example and look at it in a different way, in terms of my challenge. I read a lot about the personal communications network, and Motorola is really into that world. There are plans for all these things that are going to put a device in everyone's hand and people will get Social Security numbers the moment they're born, and then that will be the number they carry for life. And I think, "Well, that's what the military is going to use." Will that come to be? They're not going to have ITT or somebody build a separate radio. They're just going to use these things because, hell, if the STU-III worked in Desert Storm, why not take the next step and just

take these things to the next war, wherever that is? Our challenge is to get these manufacturers to put security in these things, and the challenge is that I don't have $200 million, as I did in the STU-III case, in up-front money to take the risk out of doing that on the part of companies. So that's, I think, how some of that technology will come to pass. How do we influence the designs so that they include the security features that the military will need?

Student: Depending on what you're talking about, you also have other elements of government who are working against it. For instance, the FBI would not be particularly happy if you have all these telephones encrypted, so then they couldn't eavesdrop as easily against, say, drug traffickers.

Hearn: That's right. They've got to break down more doors, use more bugs, or something. Yes?

Student: Do you foresee the necessity for having to go off-shore for your technology in the future? What difficulties will that pose?

Hearn: We already have committed that sin. We are now looking for new sins to commit.

Horowitz: I think one of the things that you and NSA should think about is the slope of the curve in terms of the certainty of security versus dollars, because in the end there will be only so much money spent on security. In the old days, the Soviet Union would have spent an awful lot to take advantage of lapses in security, whereas it's hard to imagine now who's concerned quite that much. So then, it really comes down to the slope of that curve. I mean, I've never seen a curve that says, "Gee, at half the price, you get three-quarters of the security or one-eighth the security" and I'll bet that until people understand that, they'll spend only so much.

Hearn: A spin on that, Barry, and you're right on, is to throw out our evaluation mentality of old and say, "Put this out there." We know it's flawed. We know some of them are, and in three years we'll fix them because we will roll over, and we can fix some of the flaws in the rollover version. So we'll have new ones out there, and the adversary won't have a chance to react.

Oettinger: Could I push on that just a little bit before we go on to something else? There's that book about World War II shenanigans called, *Bodyguard of Lies.*[*] I'm just wondering, you know, in the current environment whether one couldn't write a book called, "Bodyguard of Lies, Half-truths, Truths, and Overload," because certainly always in the U.S., but now increasingly in the former "evil empire" and around the whole world, the amount of stuff that's whizzing around is growing by leaps and bounds. So the job, then, of intercepting or snooping is going to get harder and harder. The odds, therefore, of hitting pay dirt when there are such tremendous amounts of noise have got to be decreasing. You know, in some absolute respect relative to the past, this question that you've raised, Barry, takes place in an environment where the raisins are embedded in a larger and larger cake. I want to reiterate his question in that sort of context. Is anybody kind of looking at that, because it seems to me that the natural protection by a bodyguard of noise is increasing, especially in the U.S., where this information sort of comes naturally. It's called journalism. Is that a factor or am I just kidding myself?

Hearn: No. This is an exciting time because of all the changes — the evil empire is gone and all that — and we are taking advantage of this. We're trying to reexamine some of the basic credos and commandments that were underlying our previous experience, Tony, and that's one of them.

McLaughlin: But, Tony, I think that gets into the countermeasures business again, and the same technology that leads to proliferation makes it easier to intercept and to search. And hark back to 1984: think of our network conference with Lee Paschall,[*] talking about what used to cost hundreds of millions to do and what he could do now for a million dollars in a pick-up truck. You're searching only for the given phone calls that you want. You don't have to look at all the others. It's only from this number to that number. SS-7 actually works against that by splitting the signal, but the hardware for intercepting, prying, and sorting gets cheaper, too, by leaps and bounds.

Oettinger: But I think that's the trouble. I just have a gut feeling that the amount of noise being generated is likely to outgrow the ability to filter it, especially given the absence of concentrated resources, such as the KGB or something. Or maybe not.

Hearn: Barry put his finger on a large factor there, the self-regulating department. As money goes

[*]Anthony Cave Brown, ed., *Bodyguard of Lies*, New York: Harper & Row, 1975.

[*]Lee Paschall, former Director of DCA and Manager of the National Communications System.

down, you're not going to be able to do so much. So you'll do whatever you can do within those bounds. And I'll think of all sorts of more noble-sounding reasons for why we're doing that between now and then. But cost is the driver.

Horowitz: Yes, but you'd like to be competent in the things you're doing, do the best you can, even with that money, which takes some sort of reevaluation of the situation. At least, my sense has been that NSA has had a very absolute view of security, which was justified because we had an adversary who could do quite a bit. But that's over.

Hearn: We are definitely trying to change our attitude. And the neat thing about it is that we have some senior people who are in the lead, which is very encouraging to me because they would be the ones one would expect to hold on to the tenets of the past. We have some of these people saying, "We've got to change," because of some of the reasons you mentioned. Yes?

Student: I'd like to know about the increasing volume of users, because I can imagine many people get to use those machines. Is there any problem of redundancy? That's the first question. And how vulnerable are fiber optic communications?

Hearn: Okay, you're going to have to help me make sure I understand your question. Are some means of communications inherently safe because they are on fiber optics? Is that the second question you asked?

Student: My second question is, is this system foolproof, sir? What is the vulnerability of the communications system? Is it safe?

Hearn: Yes, well, certainly if you send things over fiber it's more difficult to access than if you send it out by microwave radio, so there's an inherent security feature in fiber optics that's lacking in microwave radio. So, depending on how you choose to communicate, you can enhance or not enhance the security of the communications. What was the other question?

Student: The redundancy caused by an increasing volume of users. Is there any problem with that?

Hearn: Redundancy in what sense? I don't know what you mean by that.

Student: If the system fails, there is some overload of users?

Hearn: Do you saturate the system?

Student: Yes, something like that.

Hearn: There's an awful lot of capacity. You talk about system robustness in different ways, and capacity, the ability of fiber to carry gigabit-per-second rates, certainly exceeds most people's needs these days. A lot of entrepreneurs out there want to take advantage of that and entice people to buy products. I don't see anything inherent in current communications system design that says if you have so many people using them, you'll have a breakdown in the system.

Horowitz: I think the big vulnerability is in the switches. I think the individual lines of the end users may be safe, but the switches are things that are vulnerable to a point. You don't need to sit on the fiber to figure out what's going on, but someone at the switches can do a lot of stuff.

Oettinger: I think, Barry, there's a countertrend that says that more and more folks who are not certified carriers are putting in their own switches, and may or may not become targets because they may or may not show up on anybody's roster. You have, again, measures and countermeasures.

Horowitz: It's hard to know, but today there are N companies, M switches, because of packet switching. You send data out in packet switches and you don't know which switches your data is going to go to, so that the crudest guy on the block could be handling the fanciest data on the block, and the guy doesn't even know it.

Student: Sometimes, not all.

Horowitz: Not all. Maybe all in some cases, depending on the routing, so there's an owner who has no certainty of anything.

Oettinger: But, by the same token, you know, the stuff is so disassembled that sticking it back together again becomes a problem.

Horowitz: It works both ways.

Oettinger: The central message that I get goes back to one of your slides. It's a problem either way, attack or defense, and it's getting much more complicated.

Horowitz: It's getting harder to understand, evaluate, and figure out what or where you are. I think that's true.

Student: Without getting lost in the gestalt, we seem to need a preliminary security. You have to look at the security from the whole point of view,

rather than just communications security. I mean, in the United States in particular, it's too easy to hire a former worker, or work out a deal, or have this fake consulting firm collect data.

Hearn: You're right. It certainly has come across that all of you come from a very technically oriented perspective. The technical solutions to these problems are my mission. Personnel security, physical security, other kinds of things, this is distributed across the U.S. government. You have to take a holistic view in order to really have the best.

Student: How big is the threat? The Russians were a different problem and they posed a bigger threat.

Oettinger: Early on in his talk, Jim referred to the paper by Dan Knauf, which addresses that holistic question. If any of you are interested in reading that paper, it contains comments on the whole range of vulnerabilities and susceptibilities. Jim cited it earlier to put this narrower thing in the broader context of total security, whatever that might be. I remember years ago, a major New York bank that I was working with was spending a lot of money controlling access to the computer room — fancy double doors, et cetera, et cetera. At the same time, their punched cards were put out in trash barrels on the sidewalk for anybody to collect. That got engraved in my mind. You've got to pay attention to the whole thing.

Hearn: We refer to that as TRASHINT. And that's what a lot of the operating manuals have called it.

The title of this has been, or is, "Information System Security — how we got here and where we're going." I should have said that for openers, but I didn't. I hope that in some ways I have given you a sense of that. This is not to cut off any more questions, but I want to get it in before my memory turns more fleeting than it has been.

Student: Are companies aware of the need for security, especially since the government doesn't control corporate policies?

Hearn: They react in various ways. I see an example or two at Intel, where they take great pains to protect their latest application-specific IC design, including using couriers, more than one, to take it from the design place to the factory where it's fabricated. I see other companies who just assume they don't have an enemy in the world in terms of that threat to their information. It's all over the map.

Oettinger: Jim, it's a very mixed bag. If you look, there's an extensive public record, going back to the end of the Ford Administration with then-Vice President Rockefeller, who was extremely interested in these issues. He made public a tremendous amount in aid of that point, and the general reaction was, "Ho-hum." Well, his particular concern again was with the former evil empire, and so that particular thing has vanished. It's partly as John has pointed out: some of the companies make these decisions not as irrationally as one might assume. The risks are not quite the same kind of risks as you have in a military situation. You lose a bit of money, big deal! It may not be worth the cost of the insurance. You know, you don't necessarily buy as much fire insurance as long as you don't believe that your house will be on fire. You could not operate supermarkets if you try to reduce the pilferage rate to zero. And there is — I forget what the number is — it's something like 5 percent of gross that retail stores normally assume is a cost of doing business, because they can't turn the clamp tighter without making the store inaccessible, or arresting every customer. And so it's a different situation for the central government in its role of protecting the military. It would be hard to net out what each kind of company might think about its relative risk, including saying with eyes wide open, "Why do I want to protect this stuff? Because, what the hell if they steal it, big deal!" It's only money and that's somewhat different from national security, soldiers' lives, and so on. The private sector is really different in that respect.

Student: Not only is it only money, but it's probably insured. The banking industry does lots of risk abatement through insurance.

Oettinger: Yes, because they do have a lot of not only insurance, but hedges: gentlemen, if you make a trillion dollar error, you know — we can always fix it. There's a phone call between two guys who know each other and work with each other every day, so there's a little fiction in those things, too.

Horowitz: We run into a very special problem in a place like MITRE. Maybe it's something you could help us with. We have unclassified networks that are open, as any company would, but people will say that the sum of a lot of unclassified data could be considered as classified. It's a hell of a thing to have to carry on your shoulders in terms of worrying about people having access to an unclassified network, and I presume that in time these ideas will go away, but nevertheless, that's the current state of affairs. You know, we still consider the sum of a lot of unclassified data as to be potentially classified.

As yet, we have no process for judging that, except after the event has occurred.

Hearn: Yes, they make a pronouncement and then it's up to the agency or department head to figure out when he's crossed that invisible line.

Horowitz: That's right.

Oettinger: One more comment or question ?

Student: Yes, sir. My question is about the coalition warfare as a future trend, and American communications security. During the era of the Cold War, the threat was very obvious to the United States and the long-standing, established framework for alliances such as NATO worked well. In that alliance, the key word is interoperability, so interoperability was shared, including communications to have successful combined operations. But after the Cold War, as you said, the future trend will be a specific, very tentative coalition like the Gulf War, Desert Storm. But if the United States wants to establish a coalition during a very short period, interoperability in peacetime is necessary, but the enemy is unknown and the potential allies are also unknown. How do you reconcile that with the necessary interoperability from the peacetime protection of the United States?

Hearn: With great difficulty! We have that task laid on us now by our military. There are allies of long standing that I guess, under a reasonable scenario, will continue, like the U.S. and Great Britain. So you have an interoperability and a secure arrangement with them that will just continue from the past. For the allies of the moment, I'll call them, we need to have on our shelves, so to speak, a variety of solutions. Some of them will just be for the short term, whatever the duration of that alliance is, and we'll have a product that in our estimation can be used for interoperability among all the participants. But when that experience ends, then we won't use it any longer. We'll use something different for the next one. Now, it's a lot more complicated than that, but that's the essence of what we're trying to think through, and we're still in the process of thinking through that. One of the challenges is that in the past it's taken us a long time to build something that's been in place 10 or 20 years. This approach, this philosophy, would make for much shorter-term products. As I say, we would have an array of things on the shelf and use them just for specific instances.

McLaughlin: The Gulf War provides another example of how that can be done in the case of, I guess, the Syrians and the Egyptians and other Arab forces. We assigned Arabic-speaking liaison teams who brought their equipment and their keys with them to do the communications, and then they went back.

Oettinger: A U.S. person on-site, essentially being the communicator.

Thank you very much, Jim, for coming.

INCSEMINARS1992

ISBN-1-879716-16-X