INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

Data Security in the Information Age
Robert Conley

Guest Presentations, Spring 1986
Clarence E. McKnight, Jr.; Robert Conley; Lionel Olmer; Harold Daniels; Mark Lowenthal; Richard J. Levine; John Grimes; Bobby R. Inman

February 1987

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
I-87-1

Data Security in the Information Age

Robert Conley

Dr. Conley was Deputy Assistant Secretary for Advanced Technology and Analysis, and Acting Assistant Secretary for Electronic Systems and Information Technology, Department of the Treasury, from 1983 to 1985. In this dual capacity, he established a program to plan, budget, and administer the Department's information systems. Previously, he served as the Navy's Chief Scientist for Command and Control Programs, following 18 years in various assignments with the National Security Agency. Dr. Conley is currently President of Conley & Associates, Inc., a consulting service in command, control, communications, intelligence, and information systems.

The subject that I will discuss today cuts across the spectrum of the military, civil government, and public needs. The subject is information systems. This is a term in civil government similar to command and control systems in the military. Basically, it's the interrelationship of computers and communications and their applications to accomplish a given mission or function.

My emphasis will be on the Treasury Department, and information systems, in particular, as applied to financial transactions. To start with, I'm going to discuss trends and paradoxes that exist in the "Information Age" of the 1980s, affecting information security. I will highlight some of the macro influences, such as divestiture and interest rates, and their impact on our economy, particularly on electronic security.

Based on the trends and macro influences, I will address government actions that are being taken today. I will discuss what needs to be secured, and the value of it, both for national security matters and for other information. The definition of security involves a judgmental process; time and history really guide that which needs to be secured, and with computers and electronic handling of information the ability to protect the information requires new rules and new designs. I will conclude with a discussion of the systems being developed for financial security. The points that I'm raising are really electronic security oriented; I'm using financial systems as an illustration.

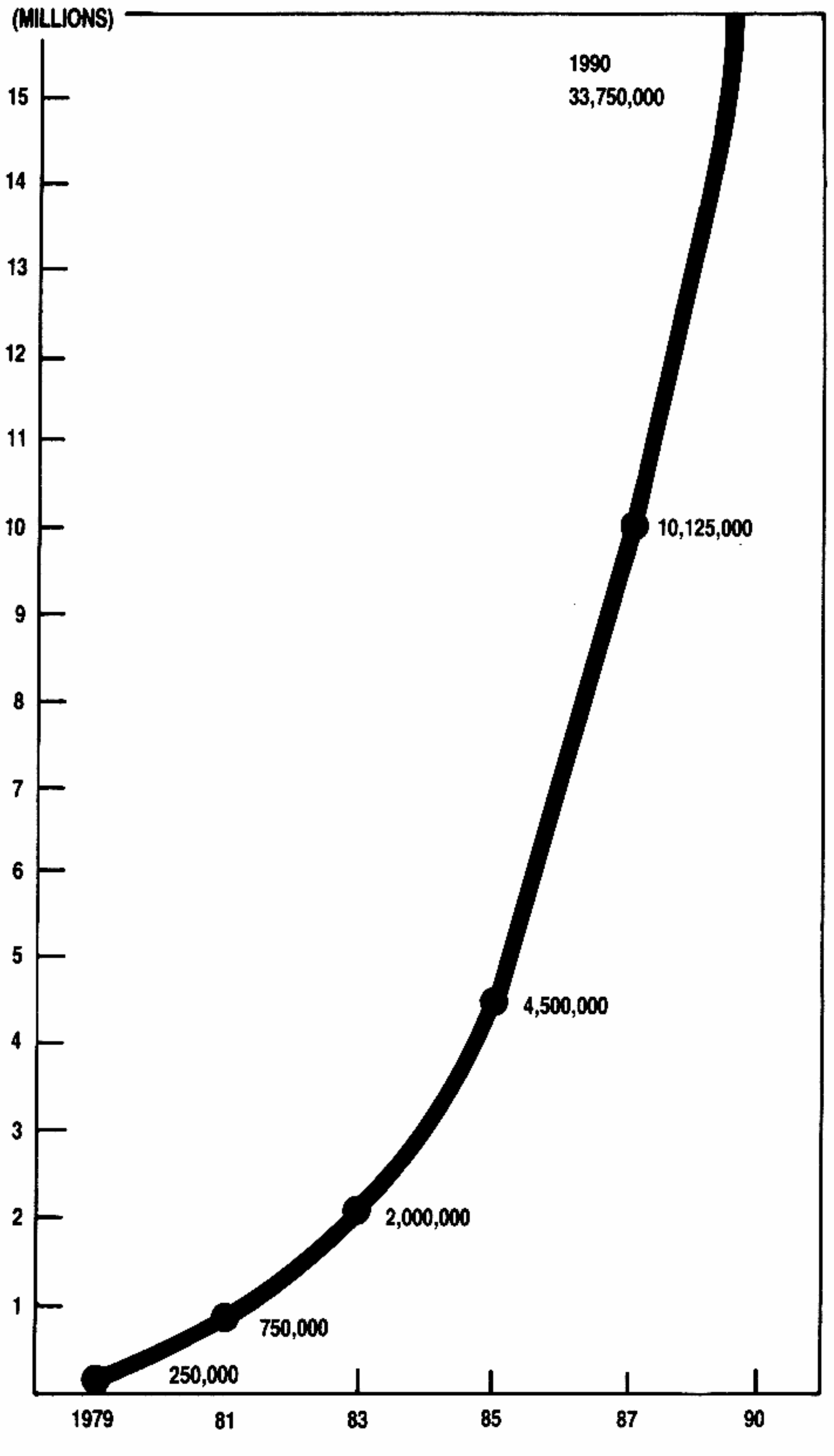
The Treasury Department is composed of 11 independent organizations (figure 1). Its mission is to collect the taxes, enforce the tax laws, and coordinate the systems for disbursement of money for the government.

Information security is the protection of information from loss, unauthorized access, or manipulation. It doesn't have to be the Soviet Union that gets the information. It could be anyone who may gain by the manipulation of or access to the information. The area of information security is a system problem. It is not just one of communications security, computer security, or physical protection alone. One must have an understanding of the overall system in order to provide any adequate security levels, and apply the techniques of security in a balanced manner.

One of the factors raising the awareness of information security is the number of low-cost personal office computers that are finding their way into our world (figure 2). This factor increases in importance when the office computers are internetted by communications. This nearly independent acquisition of

- OFFICE OF THE SECRETARY
- BUREAU OF THE MINT
- BUREAU OF ENGRAVING AND PRINTING
- INTERNAL REVENUE SERVICE
- BUREAU OF THE PUBLIC DEBT
- FINANCIAL MANAGEMENT SERVICE
- COMPTROLLER OF THE CURRENCY
- U.S. CUSTOMS SERVICE
- U.S. SECRET SERVICE
- BUREAU OF ALCOHOL, TOBACCO, AND FIREARMS
- FEDERAL LAW ENFORCEMENT TRAINING CENTER

Figure 1. Treasury Department Organizations



SOURCE: INTERNATIONAL RESOURCE DEVELOPMENT, INC.

Figure 2. Number of Low Cost (Personal/Office) Computers

office computers and the later expansion to networking present a conflict. The conflict is between the desire for networking of the various computer systems and the technological change in computer capabilities. When standards are imposed for networking information data bases, the introduction of new technology in the computer world is relegated to changes that will not impact the global system. This restricts the ability of an organization to take advantage of the technological explosion in the industry.

Another conflict in computer applications is the promised "Information Age," where information can be accessed, anywhere, anytime, from a small personal computer (PC). The paradox or conflict is found in the attitude "You can have access to all information all over the world as long as it's not mine." We're dealing with a need for multilevel security; even though computers are not designed to segregate information one from the other, we're asking the system to do just that. A security mechanism must be devised that audits users and provides access to the information.

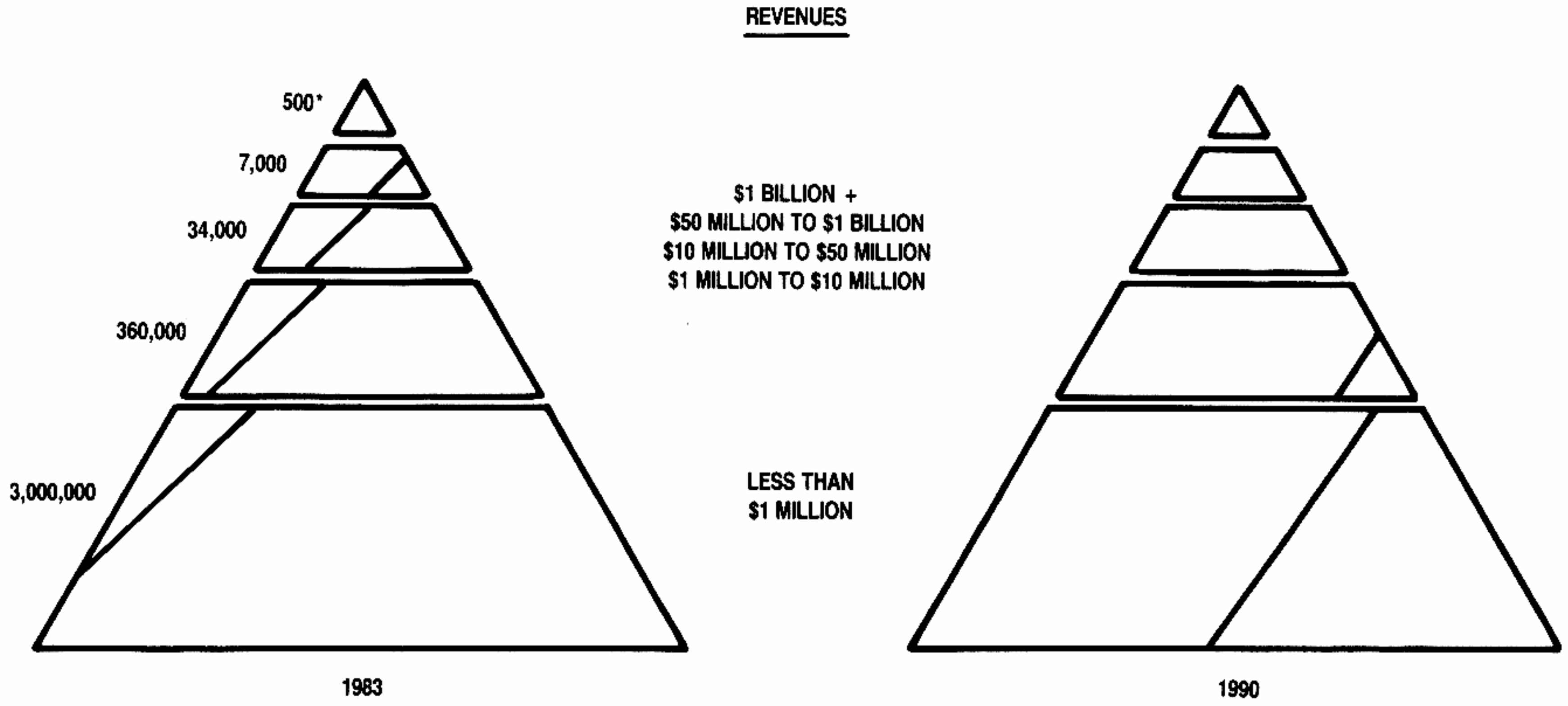
This is what is happening in the commercial world (figure 3). Estimates based upon 1983 figures from the Internal Revenue Service indicate that major corporations today are applying personal computers. Companies made large investments in computer systems and they're in the process of automating their activities. The projections are, that by 1990 the majority of corporations will be using personal computers. They will be using computer systems for a number of applications, and the systems will need to be networked to share information as well as protect it.

One of the problems that faces management is how to standardize on PCs that will provide greater productivity when networked. The price of personal computers is reaching the level of a hand-held calculator, and the controls imposed should not cost more than the resources being controlled. What standards should be imposed on the microcomputer? This chart (figure 4) gives a notional idea of the situation today. The vertical axis has cost, number of users per machine, and amount of standards and controls, while along the horizontal axis is the spectrum of computers grouped as mainframe (large), minicomputer (medium), and microcomputer (personal computer). At the division between medium and small computers there is a need for an organization dedicated to operate the computer complex — in other words, data processing centers.

To the right of the division (figure 4) is the personal computer, and the number of users per machine, cost, and associated regulation are relatively lower. Software routines for personal computers should be tested and standardized, but there are difficulties in this area. Individuals now can write their own software, with a potentially harmful result. In the military, personal computers have been purchased and placed in an operational environment with untested software routines written by a contractor or someone interested in applying the new capability who does not want to wait on the system to respond. A problem can occur when two such activities require coordination. For example, two separate software routines may be written to predict the operational range of a radar for various propagation conditions. If the software routines are homegrown there is a good chance that the prediction results will be different, and both may be in error from actual operation. When the results of the two separate software programs have been coordinated, the different predicted areas may introduce confusion and increase uncertainty in battle management.

Personal computers are becoming as cheap as hand-held calculators. People who buy hand-held computers do not consider standards. If you went to Sears and saw customers looking over all the different varieties of calculators and asked the average person why he was buying a particular calculator, he would not say, "Because it has the inverse hyperbolic sine function, which I use every Thursday," or something like that. The real answer is that he purchased it because it feels and looks good. This is the marketplace in which personal computers will exist, where variety flourishes because that which feels good or with which we are familiar is marketable. We're at the point where standards would be oppressive to the marketplace. The hand-held computer, however, has a common software or hardware equivalent that assures the user that 2 + 2 will equal 4.

So where's the problem? We shouldn't put oppressing standards on personal computers because of their variety and low cost. However, there is increasing evidence that personal computers will be interconnected by communications group software and data (figure 5). With communications sharing creeping into the process, the personal computer is now a much more powerful instrument and requires additional control to protect the group investment. When communications are introduced, the number of users sharing the overall computer assets becomes larger.



*FIGURES REPRESENT APPROXIMATE NUMBER OF FIRMS IN EACH SIZE CATEGORY BASED UPON INTERNAL REVENUE SERVICE STATISTICS.

Figure 3. Corporate Adoption of Terminal-Based Services

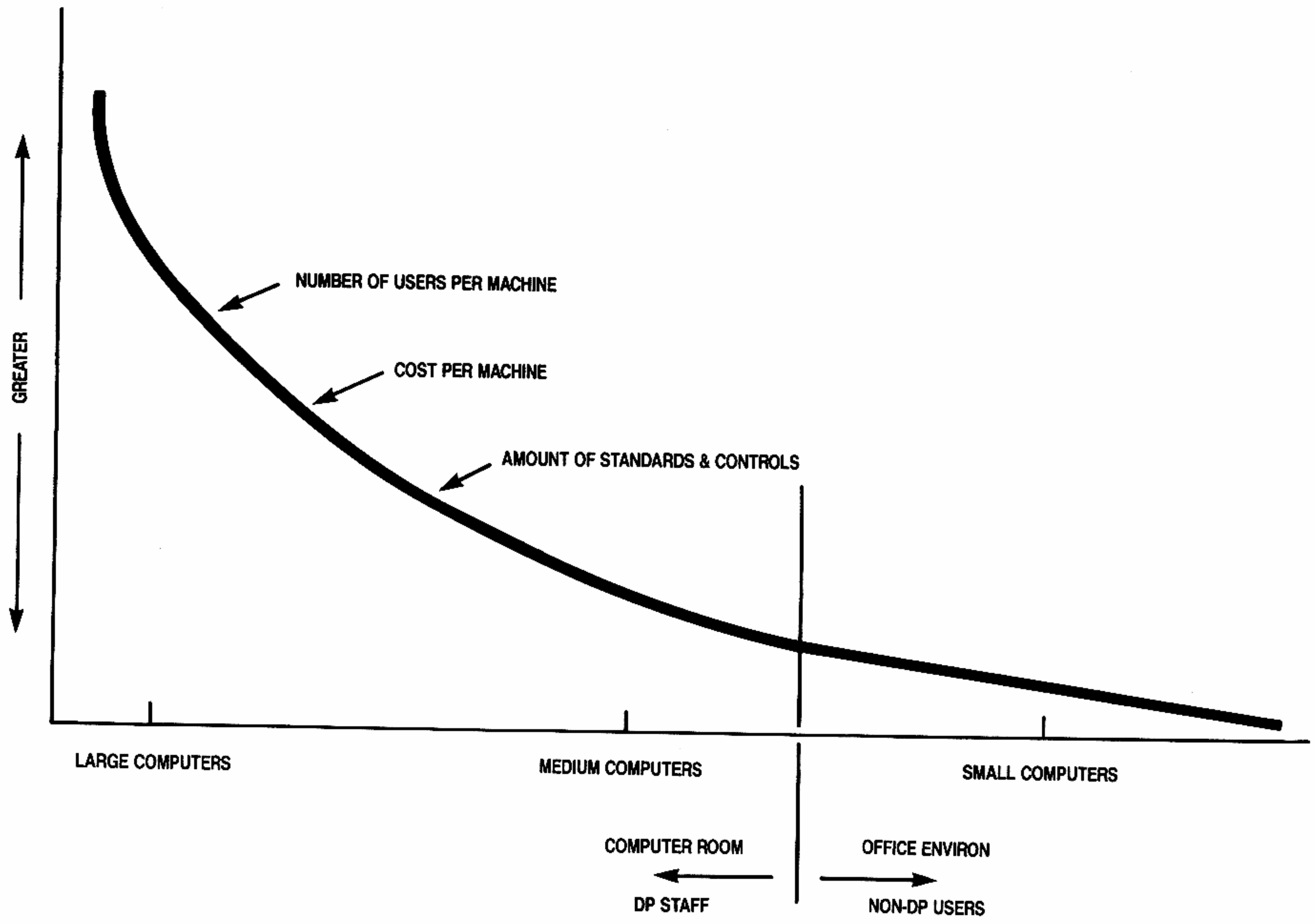


Figure 4. Past Relationships

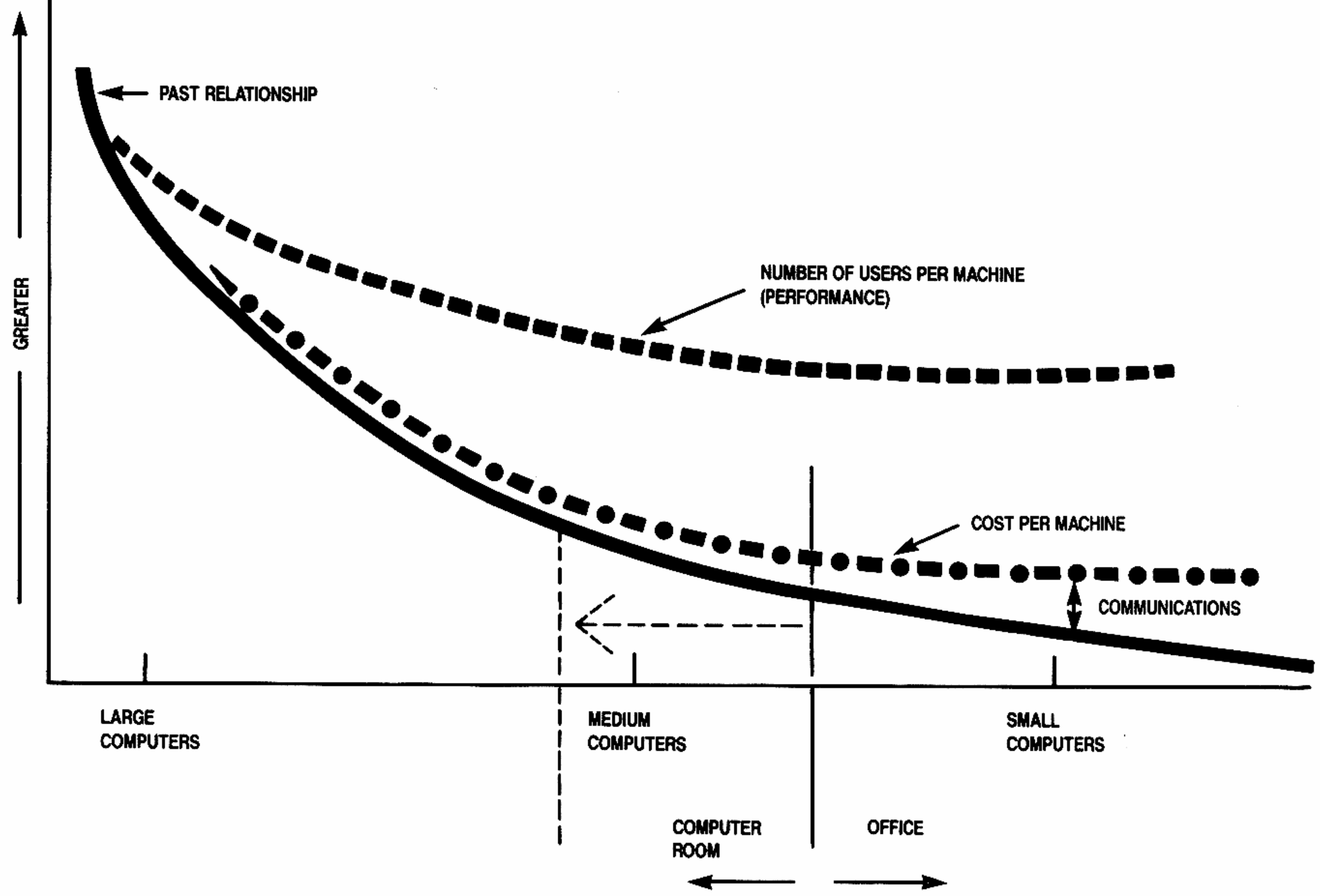


Figure 5. Future Relationships

We find ourselves in an unregulated realm of information where it can be accessed by a number of people who are not accountable. What we're heading towards, based on this projection, is a situation where people say, "Because I am not able to protect access to the information that's mine, I would like to protect the information itself."

Oettinger: When you showed us the uncomplicated version of this (figure 4), and you were down where there's very little standardization, you gave the example of the guys with their military applications and implied that their situation was bad because two different software routines could produce tracks at different distances. What you're now saying about both standardization and protection sounds to me as if you're prejudging this standardization and control issue without saying initially, "Compared to what"? In the case of the unstandardized software, maybe the distances were different but the crews were in fact detecting the targets, whereas without the damn computers they might have been waiting for the big thing that never arrived. In the case of the people bemoaning their unprotected information, without the computers that give rise to it they might not have had the information at all, and it would be wonderfully protected but also useless; or, they might have scribbled it on pieces of paper that they left floating around the lunch room or somewhere. You made a couple of statements that sounded absolute and conclusive, and I wonder if you will keep them that way or at some point mold them into a comparison.

Conley: In the example of the software, they were running computers off-line, and they actually programmed a model to predict the area of detection. I gave that as an example of a bad point where standards were needed on software and not necessarily on hardware. You have to be careful when you apply standards. The people wrote the programs using their own particular ideas of the propagation models. When the programs referenced were compared, the accuracy of the predictions was found to be lacking.

Oettinger: Is that a reasonable comparison? How good would their performance have been if they hadn't done that?

Conley: Well, the problem is that by postulating a given coverage, they can say they have sufficient coverage of an area when their range of detection is actually not anywhere near what they've approximated it to be. Consequently, they haven't swept out the area that they should sweep out. In that case it's a bad result.

I was trying to point out that at the PC level, people are experimenting on their own. The problem comes in when you try to share the results of two independent and untested predictions. To say nothing of becoming overconfident in the untested results.

Oettinger: No, but you have that problem with the kind of data that's scribbled on a notepad, in terms of what happens when you try to use it, or what happens when you try to protect it. I'm still a little bit lost as to what you are trying to remedy.

Conley: I wasn't trying to remedy anything. All I was trying to say is that even if you standardize the hardware and the machines that you're involved with, you must look at their applications and be concerned about those. I wasn't trying to say anything more than that. I was giving an example where the degree of freedom in software made standards in computer hardware less than desired.

Oettinger: You present problems, and take it for granted that they're problems. Why aren't they opportunities? Why aren't they better than some alternatives? I'm trying to get you to say "Problems compared to ...." — what? Nirvana?

Conley: The power of the PC may be more than a novice can control when the results are used for major decisions. An accountant, let's say, who is writing up a routine to figure out your income tax can become a software expert overnight. He may write a program to do the process one way and somebody else may write it some other way. What you put in the hands of the novice is power without the proper training or the proper discipline to do anything with the product. Major computer systems have dedicated people and processes for testing, which are not associated with the personal computer.

Oettinger: That's an arguable point. I find it somewhat biased toward the centralized data processing view, and a lot of people disagree. You're stating it as if it were commonly accepted.

Conley: What is it that we are disagreeing on?

Oettinger: You keep saying that things that are centralized and controlled and standards are better than things out there on the loose. I keep hearing you saying it, but maybe I'm crazy.

Student: I think there may be a refinement on that.

I think he's saying the problem is that when they're out there on the loose, on the right (figure 4), there's a problem of matching assumptions and claims of capability with actual results. Whereas when it's further back on the left, you know that the people who have those machines and software programs in their hands have some more expertise or some more knowledge about the system to make the results match the expectations or the assigned project that they're supposed to be accomplishing. It's when that project is out on the right, in the hands of people who have suddenly acquired a new capability and don't necessarily have the backup expertise, that it runs into unknown unknowns. They might not know when they're not doing the job right, and might not question the results.

Oettinger: Yes, and I guess what I'm trying to say is that, on the left, a countervailing view is that the centralized guys may get their act together 20 years down the road and produce something perfect 20 years too late, whereas the guys on the right may, here and now, do something more incoherent, but better than nothing, even though far less sophisticated than what the other guys will produce 20 years from now. I keep hearing Bob as coming out rather conclusively on the side of the centralized guys. Maybe I'm doing you an injustice.

Conley: No, I was only saying that control, and the rationale for control, are greater if separate and untested results may have significant impact on operations. There are a hundred people, let's say, using a big mainframe, and so therefore additional controls must be placed on each and every one of the users in such a way that they do not impact on the other users.

The context in which control might be applied at the PC end of the scale has changed if the results are to be shared and are to impact major decisions. If you're going to introduce security techniques, you're going to have to introduce some kind of standard on the system. I can just point out some of the complicating factors with standardization in the Washington, D.C., area alone. There are roughly 250 microcomputer manufacturers with 800 different computer models or variations and roughly 2,400 software vendors, all of whom have their own disciplines and their own software operations, as well as 160 local area network vendors. If you're trying to impose some form of standards in these areas, whether it be communications, or multilevel security, you have a problem in a competitive society.

Oettinger: That statement, Bob, neglects what a marvelous security asset that total confusion is; it works both ways. I would have a hard time getting one guy to break into all those systems. The argument for standardization strikes me as, you know, one-dimensional. Am I missing something?

Conley: I'm not really trying to make much out of this except to say that if I'm going to start imposing security requirements and restrictions on community systems, I have to be able to standardize in some way, and that standardization or controls are very difficult to agree upon today. And if I do standardize, I tend to start slowing down the introduction of new systems and changes. The obvious example is in software. If I really am going to have something that I trust as good software to sort out all the problems and make sure that nobody gets into it or out of data bases, I can't change it, because if I change it I have to test it through all of its aspects again, in order to make sure that it's still secure. I'm not making the case right now that it is an impossible problem, but I am saying that it's a problem that must be approached with caution, and that it's a different kind of problem, because we're really talking about a federation of computers interconnected by communications with limited control.

Information security, in this regard, is no longer just a computer process or just a communications process. It is a problem for the community that is sharing the information. The standards you're going to have to set will be somewhat limited or confined, or you're going to have to be content with segregating yourself from the community, in effect unplugging yourself from the network, and only working on that information to which you alone have access.

We've been discussing computer purchases by major corporations. This chart (figure 6) of the factors involved in choosing a PC shows the number two desire is connectivity. This demonstrates that the intent is to share information, but concern for protecting the information is not in question. The chart shows what people really are concerned about. The vendor is most important. The government, for example, can't do much about this. It can't specify that it wants to buy all IBM and therefore have some compatibility. Connectability is the second most important thing in their minds, again, gaining access to information.

Student: Why isn't security on there?

Conley: Well, because today's computers are not

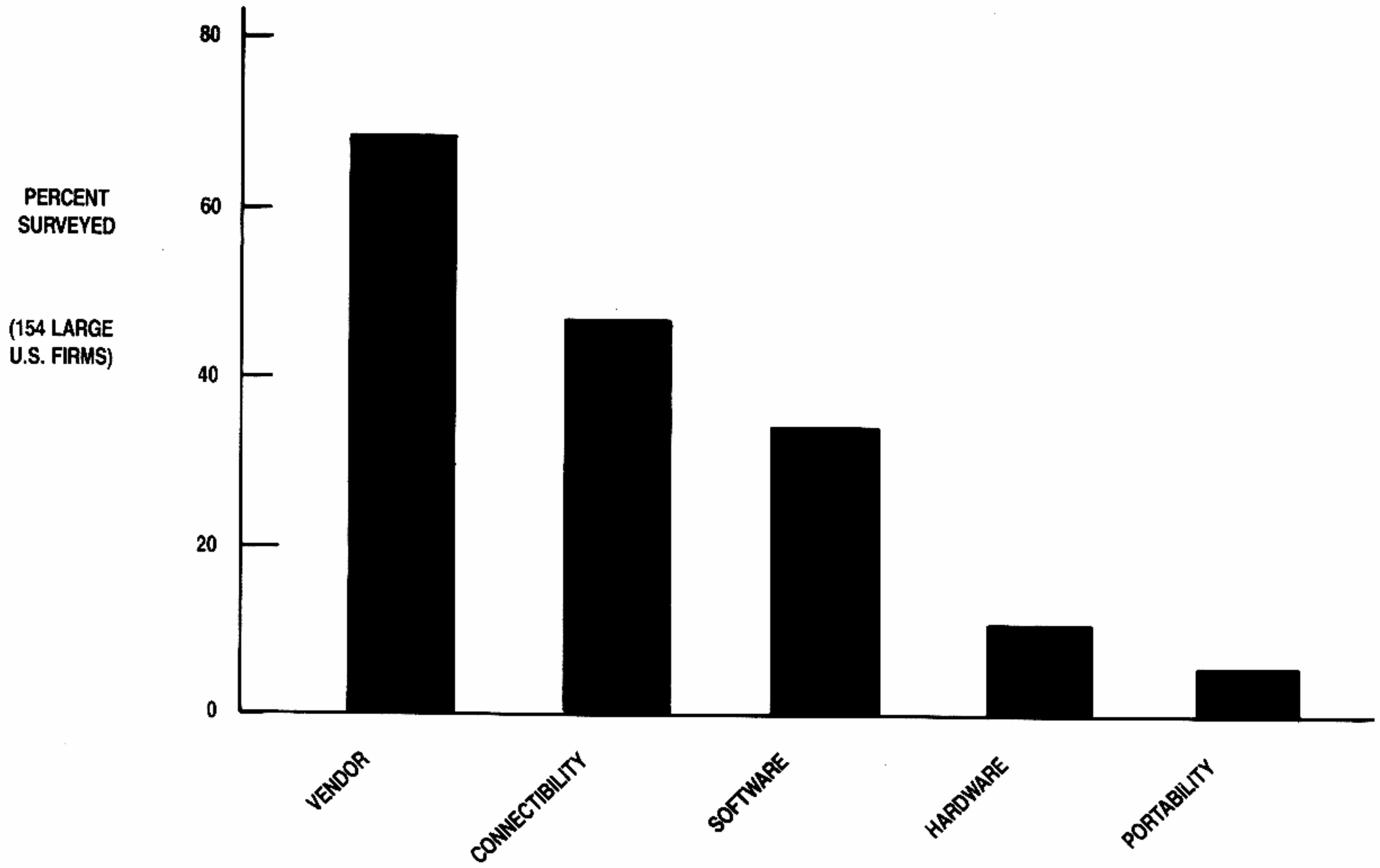


Figure 6. Major Buying Concerns

designed for security. Over the past several years, computers have been increasing storage capacity, and have been increasing access to that storage capacity. The faster the retrieval a machine has, the faster it is, in the sense of carrying out its functions; it's also easier to sell. Consequently, the machines themselves are designed to get data out as rapidly as possible, not necessarily to worry about multilevel security. The basic designs themselves don't even have that attribute.

Student: Is business concerned about security, or are you saying that it isn't? Because there isn't a demand, you don't have that capability?

Conley: I'm saying that even if you were concerned today about security and you wanted to protect your information, and you were using and sharing a machine, or a network of machines, you wouldn't have much of a chance of securing that data once you put it in, based upon today's design.

Student: And the design is a reflection of demand?

Conley: Right. We have been pursuing storage and rapid retrieval of large volumes of information. We have not been pursuing network and information segregation. It was not a good marketable function. Today we don't have the capability that we're looking for, which is the ability to share, by economy of scale, computers or computer networks, or essentially their data bases, and still segregate certain data from the other users. That's just not the way it's designed today. We've gotten ourselves into the Information Age, where we're exchanging information but with very limited hardware and very limited capability to do what we think we need to do, which is to go into some kind of multilevel security data base or information sort. The option is to use separate machines. That's the best way to go to multilevel security today.

Student: I would have thought it would be software.

Conley: No. The vagaries of software are such that you really cannot determine, or appropriately test, all software combinations. I can go through a number of examples of where that's the case. There are so many loopholes in the current designs of time-shared machines that you run the risk of not knowing if you're protected or not.

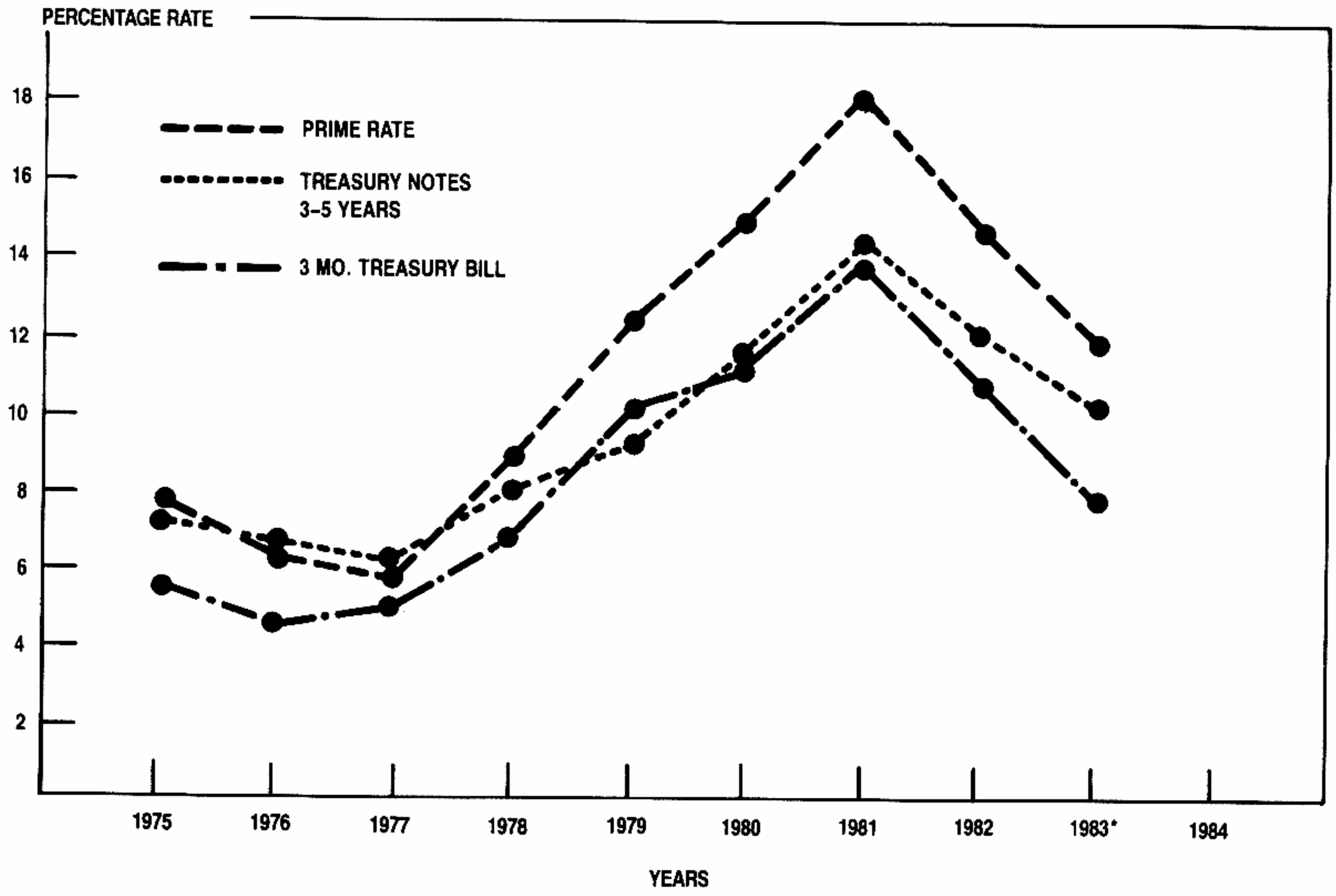
I have described some of the trends and paradoxes in the commercial base from the viewpoint of vendors and consumers. Meanwhile, the government has been growing increasingly concerned about its data bases, their loss, unauthorized access, etc. I will discuss an application of that increased awareness and its relationship to two macro influences: AT&T's divestiture and a fundamental change in the financial world.

In divestiture there was a breakup of the solidifying aspect of communications management for the government. Prior to divestiture, Ma Bell was a 100-year-old institution and working reasonably well. It was torn apart at a time when the government relied on it for about 80 percent of its communications. Now that divestiture has occurred, there are a number of different vendors who must be orchestrated independently. The user organization, in this case the government, must become more educated, and in many cases must have people available to manage its own developments and networks, or at least be able to organize the vendors. With divestiture and the fact that there is no longer a single entity for full service, the government is being forced to become more knowledgeable of its own communications assets, and in many cases to develop its own private networks.

At about the same time, there was another factor that was mysteriously stirring around in the pot of the promised Information Age. Roughly around 1981, there was a large peak in the prime interest rate (figure 7). It became quite evident, from the initiatives taken by most people, that in transferring money in the normal, classical way, such as by check, the float was large, losing 18 percent on money as it was in transit. The government made a conscious effort through cash management measures to manage the float better, and to look at electronic funds transfer (EFT). (EFT is really a misnomer; you're really transferring the ownership of that money, not the money itself.) The high interest rate was a large impetus for both the government and the commercial world to change over to EFT for improved cash management.

A lot of systems were initiated from this impetus. However, security was not a major concern when these computer- and communications-based efforts were initiated.

To give an idea of the magnitude of the funds we're talking about, the Treasury Department's annual collections in FY 1983 were $850 billion. The annual outlays were $1.1 trillion. The daily cash flow was $8 billion — roughly a billion dollars an hour is transferred in an 8-hour day. The annual security flows amounted to $2.5 trillion.



SOURCES: BUSINESS CONDITIONS DIGEST, FEB. ISSUE FOR ALL 1982, 1983 RATES.

STANDARD AND POORS INDUSTRY SURVEY, VOL. A-L, JAN. 1983 FOR 3-5 YEAR TREASURY NOTE RATES & PRIME RATE, 1975 - 1981.

STANDARD AND POORS STATISTICAL SCIENCE, APRIL 1981 FOR TREASURY-BILL RATES 1975 - 1979, JAN. 1982 FOR TREASURY-BILL RATES 1980-1981.

*TO FEBRUARY 1983

Figure 7. Interest Rates 1975–1983

To support the rationale for electronic payment systems, these are the payment methods that exist (figure 8). A check, which is the accepted method, costs roughly $2 in handling costs. In New York City there are trucks that haul the checks back and forth and distribute them among the banks. This cost factor, plus the rate of interest that is being charged at the time, is an obvious reason for implementing electronic funds transfer. As a summary, this (figure 9) shows the trend in the change of payment methods.

In the rush to automate, little attention was given to computer security, communications security, or network security of non-defense governmental systems. The laws covering electronic theft are not even up-to-date. Laws associated with theft in matters of national security carry a $10,000 fine or 10 years' imprisonment or both. The law today is not written for electronic crime. The legal aspects of the whole world of information flow, whether it be military, civil government, or commercial, really constitute a challenge for areas of law, economics, and criminology that will evolve.

This chart (figure 10) shows the results of prosecution in the past. These numbers were based on a small sample, but they nevertheless show an imbalance in prosecuting electronic crimes, whether or not they involve national secrets.

I don't want you to get the idea that protecting this kind of information is any different from national security measures. I do want you to get the idea, though, that there is no governmental entity today that gives you consistent guidelines or rules on how to protect this kind of information, whether it's your tax return in an electronic form, or your own information.

Now, the reason I need to discuss the proliferation of PCs is because the most troublesome current and future aspect of computer crime happens to be the proliferation of computers, based upon a report on computer crime by the Task Force on Computer Crime, Section of Criminal Justice, American Bar Association (figure 11). This table gives you the reasons why the government, as a whole, is concerned. The lack of adequate security measures is a primary reason. The lack of any general guidelines as to what should and should not be protected is also a concern.

What motivates the computer criminal? It is not the same thing as in crimes involving national security; it's really personal financial gain (figure 12). Obviously if a criminal saw the earlier comparison of the penalty facing a traditional bank robber versus that facing an electronic bank robber, he'd want to have a computer right at hand. As for the intellectual challenge, I believe there was a case just a few days ago where an individual was caught breaking into a number of files.

These are the most significant types of computer crime going on today outside the national security realm (figure 13). Theft of assets is a big one, and I'll get to it later. I'm sure you've all heard of the software programmer who programs the software to suddenly die on his day of retirement. That's vandalism.

Student: People aren't actually stealing data, then; they're modifying it?

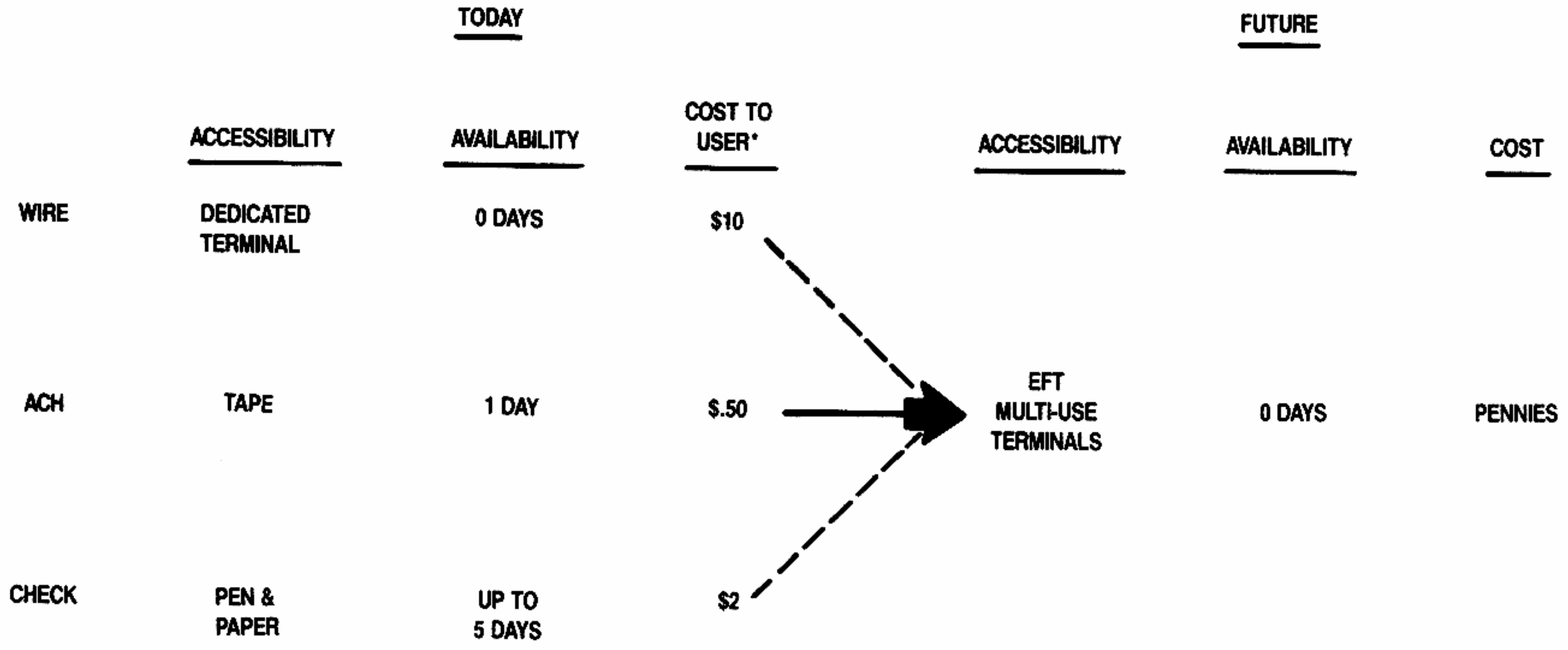
Conley: Yes, that's one of the concerns. It's possible that modification of data may be a crime equal to theft of funds. There is nothing wrong with accessing data electronically. But, if the data is manipulated and a user expects accuracy, the results could be harmful. Weather information is an example. The manipulation of data should be a crime today, equal to that of taking the data out and using it for other purposes, whether or not the value is directly associated with the transfer of money. But again, that's part of the problem that will require legal resolution.

Who has the primary responsibility? This is kind of an interesting chart (figure 14). It's another way of showing who has the information that should be protected. Private industry has almost 50 percent of the data or information floating around in the community today. The government has a 10 percent problem, but it has the responsibility to the general public, the largest customer.

These are the steps being taken today (figure 15). The Department of Defense has had a long history of being able to protect information, but mostly in the area of communications security (COMSEC). It is now investing a considerable amount of resources in computer security (COMPUSEC), and the government is also taking policy action in the form of a National Security Decision Directive (NSDD 145).*

NSDD 145 did several things. First, it said, "Do not just consider security of computers or security of communications — combine the two." Prior to that

*National Security Decision Directive 145, *National Policy on Telecommunications and Automated Information Systems Security*, September 17, 1984.



	TODAY				FUTURE	
	ACCESSIBILITY	AVAILABILITY	COST TO USER*	ACCESSIBILITY	AVAILABILITY	COST
WIRE	DEDICATED TERMINAL	0 DAYS	$10			
ACH	TAPE	1 DAY	$.50	EFT MULTI-USE TERMINALS	0 DAYS	PENNIES
CHECK	PEN & PAPER	UP TO 5 DAYS	$2			

*COST TO USER REPRESENTS APPROXIMATE COST INCLUDING CHARGES AND INTERNAL ISSUING COSTS

Figure 8. Payment Methods — "Collapsing Universe" Perspective

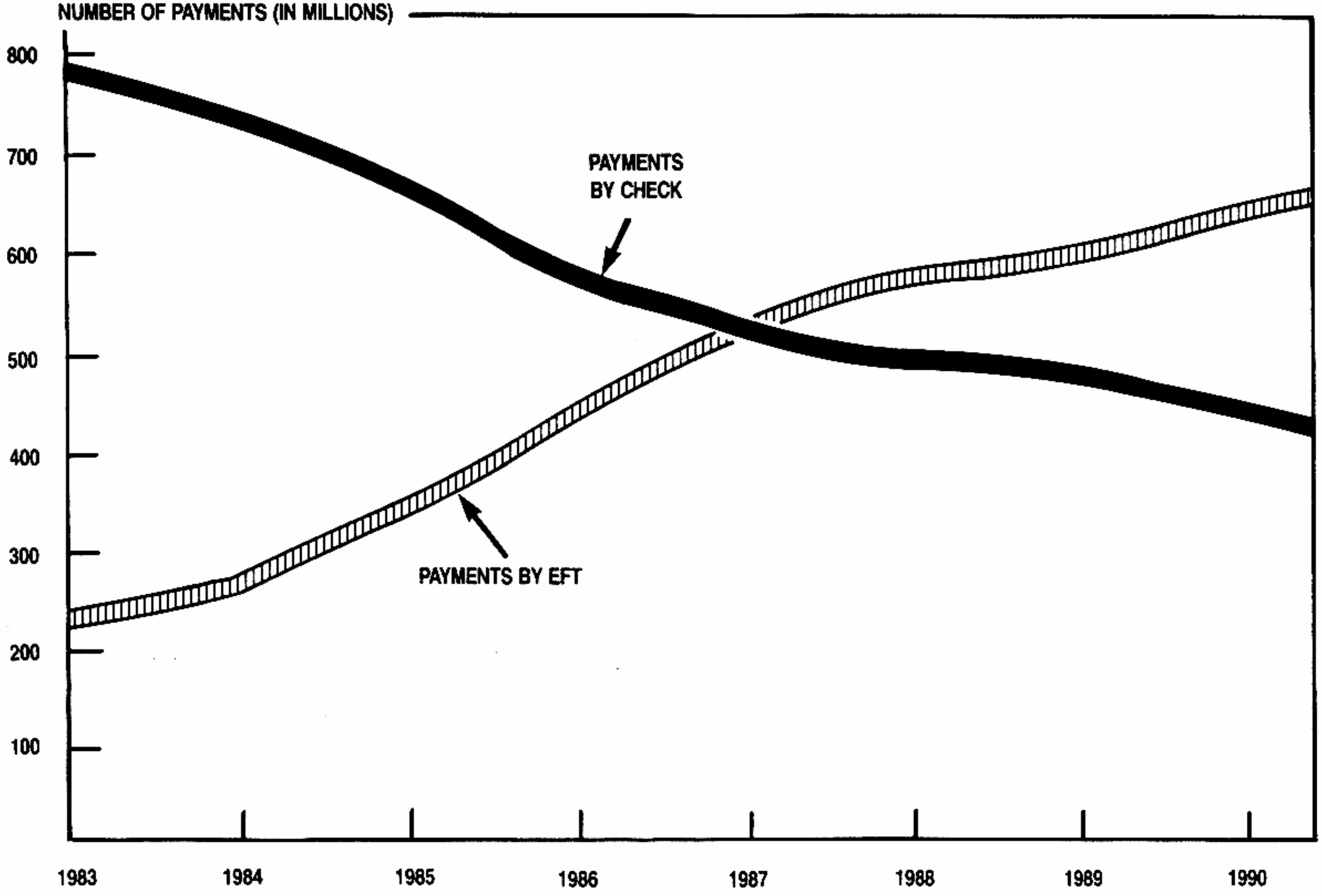


Figure 9. Change in the Method of Payment 1983–1990

	AVERAGE AMOUNT OF THEFT	PROB. (JAIL) IF CAUGHT	LENGTH OF SENTENCE
BANK HOLDUP	$20,000	90%	4 - 6 YEARS
EFT CRIMINAL	$500,000	15%	4 - 6 MONTHS

Figure 10. Results of Prosecution in the Past

• PROLIFERATION OF PCs	23%
• DIFFICULTY OF DETECTION	21%
• LACK OF ADEQUATE SECURITY MEASURES	20%
• LACK OF PUBLIC/MANAGERIAL AWARENESS	14%
• INCREASING RELIANCE ON COMPUTERS	11%

SOURCE: REPORT ON COMPUTER CRIME - TASK FORCE ON COMPUTER CRIME,
SECTION OF CRIMINAL JUSTICE, AMERICAN BAR ASSOCIATION

Figure 11. Most Troublesome Current and Future Aspects of Computer Crime

---

• PERSONAL FINANCIAL GAIN	96%
• INTELLECTUAL CHALLENGE	62%
• OTHER PERSONAL REASONS	35%
• ORGANIZATIONAL/CORPORATE FINANCIAL GAIN	25%
• DESIRE FOR PUBLICITY/RECOGNITION	15%
• ORGANIZATION PEER GROUP PRESSURE	11%
• EASE OF ACCESS/FINANCIAL GAIN, ESPIONAGE, VANDALISM, ETC.	7%

SOURCE: REPORT ON COMPUTER CRIME - TASK FORCE ON COMPUTER CRIME,
SECTION OF CRIMINAL JUSTICE, AMERICAN BAR ASSOCIATION

Figure 12. Motivation of Computer Crime Perpetrators

• THEFT OF ASSETS	87%
• DESTRUCTION OR ALTERATION OF DATA	79%
• EMBEZZLEMENT	73%
• DESTRUCTION OR ALTERATION OF COMPUTER SOFTWARE	68%
• DEFRAUD CONSUMERS, INVESTORS OR USERS	66%

SOURCE: REPORT ON COMPUTER CRIME - TASK FORCE ON COMPUTER CRIME,
SECTION OF CRIMINAL JUSTICE, AMERICAN BAR ASSOCIATION

Figure 13. Most Significant Types of Computer-Related Crimes

• PRIVATE INDUSTRY	43%
• INDIVIDUAL USERS	33%
• FEDERAL GOVERNMENT	10%
• STATE AND LOCAL GOVERNMENT	5%
• OTHERS	9%

SOURCE: REPORT ON COMPUTER CRIME - TASK FORCE ON COMPUTER CRIME,
SECTION OF CRIMINAL JUSTICE, AMERICAN BAR ASSOCIATION

Figure 14. Primary Responsibility for Controlling the Incidence of Computer Crime

• LIMITED ACCESS TO COMPUTER PROGRAMS, LOGIC	85%
• LIMITED ACCESS TO COMPUTER OPERATIONS	81%
• FREQUENT CHANGES OF ACCESS CODES, PASSWORDS	72%
• LIMITED ACCESS TO INPUT OF DATA	71%
• LISTED IN OTHER CATEGORY	12%
- COMPREHENSIVE COMPUTER SECURITY POLICIES/PROGRAMS	
- EDP/INTERNAL AUDITS	
- SECURITY SOFTWARE	

SOURCE: REPORT ON COMPUTER CRIME - TASK FORCE ON COMPUTER CRIME, SECTION OF CRIMINAL JUSTICE, AMERICAN BAR ASSOCIATION

Figure 15. Steps Taken to Prevent/Deter Computer Crime

time they were separate, and they were principally national security related. The second thing the directive did was to broaden the range of people in government who would be involved, particularly on the civil side. The Treasury Department became involved, as well as the Department of Justice, and also the Department of State.

NSDD 145 laid the ground rules, at least in a committee sense, for the participation of all the government bodies involved. It put together a community to work out the policies and the structures of what they're going to do to protect information in terms of both computers and communications access.

Oettinger: That was the Systems Security Steering Group?

Conley: Yes. The Systems Security Steering Group now includes civil government representation.

Something else happened in 1984. Back in 1963, in the process of trying to establish cohesive communications for the government, there was an organization created called the National Communications System Organization (NCS) made up of these member organizations (figure 16). The purpose was to be able to restore critical communications for these principal organizations in cases of major disasters, especially in cases of war. In 1984, by Executive Order,* this group was expanded to include the civil side of government. In a particular kind of a crisis, perhaps a major earthquake, you'd want to be able to access the information at the Census Bureau. So the NCS has now started to bring in the civil side of government. As Tony was pointing out, command and control systems, with their attributes of security and reconstitutability, are now going government-wide, and the two decisions I just outlined are the basic policy steps that are being taken.

In light of what I described before as some of the pressures and trends that are upon us, you can begin to see some of the problems the government is facing. As a short summary, combining the trends, security is becoming more and more of a problem as the amount of automation and data being shared is growing both inside and outside government; the reason for that growth is obviously commercial or monetary benefit. We need to develop a comprehensive system security program for the entire government. Moreover, one would like to have, government-wide, some reasonably agreed-upon definitions of categories of information that should be secured.

For the most part, these guidelines and definitions don't exist today. For example, it is not clear whether anyone knows what constitutes the government communications system when you take the government as a whole; it's a mixture of public and private networks. To say what it is, and therefore to say how the information is being passed around the Continental United States among government organizations, is not a simple task. As a matter of fact, it's quite difficult.

When it comes to determining the categories of information that need to be protected, there's a lot of guidance given, but the legislation on protecting information is in a state of flux. Various Office of Management and Budget (OMB) circulars have criteria on what information needs to be protected. There is also the Freedom of Information Act, which says you must have access to all your information. Given these various guidelines, one of the first things that each department must struggle with is the very question of which categories of its own information it will protect. It is the responsibility of the department head to make that decision. Basic agreement is starting to converge on definitions of what information should be protected. The breakdown is in three categories.

The first category is that of national security. The classic categories for national security information are confidential, secret, and top secret. Those really are variations on a scale of the degree of impact on national security. If information has grave national security impact, that's top secret. If it has just some impact on national security, it is classified as confidential. So one category of information for the government as a whole is that related to national security. If information involves the national security, you must protect it in accordance with its impact.

The second category of information electronically available to us today exists in the public domain. It's information that should be readily available to the public. The Patent Office, for example, is going into a system in which they retrieve patents electronically. There's no reason why I shouldn't be able to do a patent search from the West Coast as well as from Washington, D.C. There are a number of documents that are going to be electronically available as opposed to being circulated in the normal book form.

If information is in the national security realm, you and the government must protect it. If it's in the

*Executive Order 12472, 49 FR 13471, *Assignment of National Security and Emergency Preparedness (NS/EP) Telecommunications Functions,"* April 3, 1984.

ORIGINAL AGENCIES (1963)

DEPARTMENT OF STATE
OFFICE OF THE SECRETARY OF DEFENSE
DEPARTMENT OF THE INTERIOR
DEPARTMENT OF COMMERCE
DEPARTMENT OF TRANSPORTATION
DEPARTMENT OF ENERGY
CENTRAL INTELLIGENCE AGENCY
GENERAL SERVICES ADMINISTRATION
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
FEDERAL EMERGENCY MANAGEMENT AGENCY

NEW AGENCIES (1984)

DEPARTMENT OF THE TREASURY
DEPARTMENT OF JUSTICE
DEPARTMENT OF AGRICULTURE
VETERANS ADMINISTRATION
OFFICE OF THE JOINT CHIEFS OF STAFF
NATIONAL SECURITY AGENCY
NATIONAL TELECOMMUNICATIONS INFORMATION ADMINISTRATION
FEDERAL COMMUNICATIONS COMMISSION
FEDERAL RESERVE SYSTEM
U.S. POSTAL SERVICE

Figure 16. NCS Member Agencies

public domain, you must allow the public to gain access to it electronically. Public information, however, must be protected from unauthorized manipulation. That is, if a government entity is going to provide information to the general public and it is in the public domain, they must have access to it, but that governmental entity must ensure that the information is not manipulated. We should be able to provide that information and protect its accuracy.

The third category is called "sensitive." It consists of information that has to be protected either because there is a law that says so, or because there is some rule or regulation stating that it would be an infringement of someone's personal privacy if that information were to be given out to other parties. How to protect the information is another question.

Student: Could you pinpoint an example of sensitive information?

Conley: Your income tax form is sensitive, but the responsibility for its protection lies within the Internal Revenue Service itself.

Oettinger: Advance information on the discount rate being set by the Federal Reserve Board is not protected under any national security classifications, but it is sensitive in the sense that an advance leak of that information would provide an enormous opportunity for messing around with the financial system.

Conley: I'll give you another example of sensitive information. In the case of the military, they have a lot of communications security equipment. It's probably too expensive for the civil side of government to work with. But, among the people who are now doing the drug enforcement operations in Florida, there are cases where these law enforcement people need to secure their communications coordinating operations.

Now, going to Congress and saying I want money to secure those radio communications is not an argument for protecting national security. It's for possible protection of the enforcement officer's life.

There was another case of sensitive information, where a TV news broadcaster with the camera on said, "We are here because the President is going to be coming out this door in a few minutes. We have that upon good authority because our personnel staff have been monitoring the presidential communications and this is where he is going to come out." He stood there thinking for a while, and then he said, "On the other hand, if he is monitoring our staff's communications he is probably going to come out another door because he already knows we're at this door."

Authentication is an important area of security — in other words, you want to know that I'm really the person who sent or originated a message. Can the process constitute a legal electronic signature? The laws we are using right now were written in the absence of electronic signatures. We are not at liberty to say that electronic authentication constitutes a legal signature. However, from a cryptographic standpoint, if I am the only one who has a key for the code and I've put the encrypted word in my message and then you decrypt it, that coded word performs the same function as a legal signature. That's an example of using cryptographic techniques that I would say are needed in the government.

The IRS wants to start collecting your tax forms electronically. They are now sponsoring that on the commercial side, with major companies. You can send in a floppy disk. The question is, how does the IRS certify that the floppy disk came from you and that you are then liable for what you have submitted as a filing? There are a number of cryptographic questions that are going to have to be addressed government-wide, so that information is protected and certified. The problems will continue to grow. We should see, over the next decade, a lot of security techniques being introduced into government for protection of sensitive information and validation of users.

I'd like to talk a little bit more about the value of information. The value of information will be what determines whether or not one should protect the information. In the case of electronic funds transfer, the value of information is easily understood. It is the value of the transfer. The banks today recognize that, and they are going to impose some form of authentication on their electronic funds transfer. But they have a unique kind of a situation. They have customers whom they must satisfy. They look at what it costs them today to carry out what would be a reasonably secure type of disbursement of funds, and may make a judgment that it is not worth securing any further.

The logic goes something like this: You have automatic teller machines where you put your card in and get money out. You have a password, but it's really easily broken. Banks look at the population banking with them, and they say, "Okay, roughly 10 percent would cheat if given the chance." Of that 10 percent there are probably 5 percent who will attempt to steal. To account for that 5 percent of the population the banks limit the maximum per day that can be taken by machine, say $200, and cap their losses. Consequently, the operating revenues estimated for doing business electronically include the predicted loss. In other words, they build in the cost of operating to pay for the loss by fraud.

Anytime this situation is reviewed, security costs will have to be cheaper than the projected loss without the security measures. Before anybody starts securing things in the banking system, it's got to be balanced with the protection provided.

In cases concerning national security, the information is priceless; that's why a lot of money is spent to protect it. When you get into a nebulous category of what price the IRS should pay to protect your records, that's a different story. What cost is going to be associated with the protection and whom are you protecting it from? What is the magnitude of protection? Should it be protected in such a way that nobody could ever break into your IRS record for seven years? Again, it's going to come down to the two factors of cost and magnitude of protection: how much to spend and for how much protection. There are a lot of complex legal, technical, and economic issues that we face as we grow in the information society.

Student: I'd like to go back to your example of banks calculating their need for security based on how much is likely to be stolen. Do banks realistically also calculate a value for reputation or their image as a secure place to leave your money?

Conley: Image is obviously important. It's kind of an easy thing for a bank to provide a bank vault. They will spend money to buy a bank vault, because when you walk into the bank you see it. It makes you feel comfortable. But because individuals do not see electronic funds transfers, they do not have the same commercial return. It's also one of the reasons why, the law being what it is, the electronic criminal gets away with a lot more. If I were to do an electronic transfer of funds, let's say from one bank to my own bank, and the bank knew that I had done it, and they wanted to prosecute, they would have to take me to court and admit that their system is vulnerable; and not only that, but they would have to explain just how vulnerable and how I did it. If they did that, (1) they would lose an image, so they wouldn't prosecute, and (2) they would also be giving other people ideas on how to rob their bank. So they're finding themselves in an awkward situation, and when the amount of money gets large enough they will really be in trouble.

Student: It's very surprising that all these security measures are not incorporated into electronic funds transfer as much as we would like. One would imagine that banks, being in the forefront of providing security for money deposits, would be extremely careful and sensitive to these requirements. I would have expected far greater advances and developments by banks than, say, by the government.

Oettinger: Do you believe that your signature is verified every time you write a check? I think you've missed the point of what Bob said. The image situation is one situation; that's one factor. But another factor is the amount of money. As he pointed out earlier, for some things it is better to take the risk because it's too damn expensive to protect. It's just clerically much too expensive. The risks are not that great and so they take a loss. You are of the notion that somehow security is black and white — either you have it or you don't. That's a very bold assumption to make. That's the whole point. In order to have a device that is worthwhile it's got to be cheaper than the amount that the banks are willing to lose. The image thing is another factor; it may outweigh that calculation. There are a number of factors. But there's no such thing as either an absolute desire for security or an absolute achievement of security. I think much of the discussion of this subject is clouded by the assumption that somehow things are black and white.

Conley: That's exactly what I'm trying to say.

Student: The reason that I brought up banks is that, just as banks treasure their image, I think governments also treasure their image as custodians of public money. It would be very difficult, even more difficult, for the government to exercise this cold-hearted, cost-benefit analysis where they'll only go so far to enforce security if it's worth that much more, because over and beyond the actual losses or the expected loss there is this very intangible and very important factor of image or responsibility for public funds.

Oettinger: How many people a year are killed on highways?

Student: I think 50,000.

Oettinger: We are not willing to pay the price for air bags or other things that might reduce that 50,000 to 25,000. We could make all automobiles padded tanks. Yet, while on any dimension I think human life is sacred, it doesn't matter here because we want to drive and we're not willing to pay beyond a certain point for making driving safe, and we're not willing to lock up everybody caught for drunk driving because then 90 percent of the population would be in jail. Again, it's a matter of degree.

Conley: We're introducing into our very social system certain things that will have to be, but that the social system doesn't necessarily want to accept or pay for.

Authentication is an interesting term. It uses a technique based on cryptography. Let's say I have a message to send which will put a million dollars into Tony's account from my account. It goes from, to, and it gives the amount. At the end of the message there is something added that's called a message authentication code (MAC). When I prepare a transfer, the system actually runs the message in the clear into a device that takes all the characters in the message, or those that are in a selected format, and generates this tag which is added to the clear message. The clear message is sent plus the tag. The receiver of the message takes the clear text and, using the same code, generates the tag for comparison. If it's identical the receiver knows the message was not tampered with and the correct code was used to produce the tag.

The banking industry has been working for seven years on a standard for authentication. Unfortunately, it has not received wide acceptance. There's no manufacturer willing to put a million dollars into developing this device, because he doesn't believe the banks are really going to install it. Now the Treasury Department has said it is going to do it. We're talking about a cheap solution, and one that has got to be socially acceptable to the environment into which it's being introduced.

Oettinger: We are just in the middle of this transition; it's very hard to see all the details. I commend to you a book called *From Memory to Written Records*.* All the points that Bob just made are sort of covered there over a 300-year span between 1066, with William the Conqueror coming into England, and around 1300, with the transition from oral record keeping to written record keeping. Authentication circa the time of William the Conqueror involved one kind of technology: When you brought on the evidence you brought in a knight who took an oath to speak the truth and nothing but the truth, and if you didn't like his evidence you literally put his feet in the fire and you got somewhat different evidence. Those were the rules of authentication with oral witnesses.

By the year 1300, most contracts were written, and one of the ways of authenticating them was to write them out twice on a piece of parchment — text here, text there, with what was called an indenture, a very elaborate cut in between, so each of the contracting parties would have a piece of the record. The authentication process was to put the two pieces together. Simpleminded. But it took over 200 years to get all of that technology developed, socially accepted, enforced, standardized, etc., etc. And among the complicating factors was that, in the transition from having all your records in somebody's head, transmitted by oral tradition, to writing them down — much like going from paper and checks and so on to electrical messages — the question arose, what do you write down? Aside from a little fallibility in going from the oral to the written, there was also the political question of whether the Anglo-Saxons wanted to "fess up" to the French-speaking Plantagenet types, who had come over from Normandy with William the Conqueror, all the details of what they thought they had.

You get a picture there, in retrospect, of some problems that translate very easily to some of our dilemmas today.

Conley: We are certainly in the midst of a messy transition, where we're not moving evenly on all fronts. The information I'm talking about, whether it has value associated with money or whatever, is the same information that is being passed under national security guidelines, rules, and regulations. The processes for protection are much better spelled out and the penalties are much clearer in the Department of Defense.

Student: What agency in the government is responsible for that better spelling out of the penalties and the rules and whatnot?

Conley: Congress will develop the rules, but then they'll be tested in the Justice Department to hone them down.

*M.T. Clanchy, *From Memory to Written Records in England: 1066–1307.* Cambridge, MA: Harvard University Press, 1979.

Student: Is that being neglected, as your presentation implied, or is it just that it's so complicated that it's going to take a long time, as described in Tony's account?

Conley: They're holding hearings today on what is secure and what is not, what protection needs to be taken, etc. They are setting down some guidelines.

Oettinger: Who is "they"?

Conley: The Congress.

Student: Is it the Banking Committee?

Conley: Not at this time.

Oettinger: Well, you said right at the beginning, and it's something I agree with, that security is a system problem, not a piecemeal problem. The systems we're talking about know no boundaries. They involve people, communications systems, computer systems, agencies, and private sector groups; they're sort of messy things that cut around and across such divisions as public/private, domestic/international, military/civilian, government/private sector, etc., etc. Every one of the organizations that we're talking about that might do something about the problem is just a piece of that larger complex, and has its own interests and so on. It might be illuminating if you would speak a little bit about the relationship between the unitary, indivisible character of what you describe as a system problem, and the necessarily fragmented character of the people and institutions that are criss-crossed by these systems.

Conley: It is accurate to say that there is no system organization today that can orchestrate this in a unified fashion. I won't go into the diversity of the organizations, but OMB has the responsibility for oversight when anybody buys computers or communications equipment, to make sure that they take security into proper consideration. Of course, the OMB people are not the security experts of this nation. The National Security Agency has cryptographic responsibility for the protection of this nation. They are supporting the Department of Defense, primarily. The National Bureau of Standards is responsible for standards that interface with the commercial world and for the current digital encryption standards. The Department of Commerce is responsible for communications, coordination, and interface. There are a number of organizations that are responsible for various parts and pieces. One of the reasons why NSDD 145 was written was to obtain some common ground of understanding.

Oettinger: Under a committee structure?

Conley: Under a committee structure. It is typical of any problem that is multifaceted, such as this one, that you will relegate it to a committee and then ultimately, when it becomes reasonable and socially acceptable, you will administer it through a more responsible organization structure.

Student: What is the bureaucratic genesis of NSDD 145? What is it driving towards in the bureaucracy?

Conley: Recognition of the boundary crossings of areas of security is a good step forward. Recognition today that a lot of our information systems are being accessed freely by the Soviet Union and other countries, information that we have labored hard on. Recognition that we have to do something in the overall system sense as opposed to doing it separately.

One of the interesting things is that you have only so much money with which to secure your system. I would like to be able to find some way to divide that out nobly; I would like to spend the same amount of money protecting my communications as I do protecting my computer, as I do clearing my people, as I do putting a lock on the door. Is there a balanced approach to the security of the overall system? I would like to be able at least to assess that problem. You find that assessment very difficult because you have to go to separate organizations for separate solutions, and every one of them will err on the side of making sure that they're secure, which says you will have to pay the most for every one of them and you won't put it in proportion to the overall system allocation. You just need a balance and an understanding of these things.

The expenditure problem is one part. And then there's the problem that Tony alluded to: Today different government agencies are using different computer systems that are literally joined; although normally operating independently of each other, they are also sharing data, like payroll and personnel records. Now, they have to budget separately for the money to get fixes to that kind of system, and probably none of them is paying for the communications. Somebody else has the budget for that. There are at least three budget processes that are going to apply to this process. There isn't enough money even to upgrade the computer complex, let alone to do something about making the system secure.

We're dealing in the real world of a diversified problem. One of the problems, the major problem, is just plain education. People do not realize how vulnerable the systems that exist today really are. Those who are not cast in the normal Department of Defense mold are simply not aware.

Oettinger: The phenomenon is not unique to this area. If you think of the number of people who have died or come close to dying in high-rise office buildings, you realize that the toxicity of smoke generated by modern plastic materials is not something that burst on the consciousness immediately or was recognized immediately in building codes. The recent Prudential fire here in Boston is an example — no sprinkler, not enough smoke alarms, etc., etc. — and it's a miracle that it turned out to be sort of a benign one, but there have been earlier ones in New York that were much more vicious. It takes a period of time for the insurance companies to require greater protection before issuing or writing a policy. Yet, as you can see with the doctors and the malpractice suits, there comes a point again where we lose the balance between the goal and the cost of achieving it. It's hard to get obstetric care in Massachusetts right now because the doctors are striking and screaming, and if you want to have prenatal care you have to go to a midwife because the cost of malpractice insurance has gone up so high.

What you're witnessing in the data area is a pervasive phenomenon as to how much money you're willing to pay for protecting something against a stochastic risk, and you may not want to shell out a lot of money when you're not the one who's burning in the high-rise building.

Student: Don't you pay a penalty in speed, accessibility, and flexibility with any kind of computer security system? If you put a good one in at the bank, aren't the customers going to take longer to get their things done and have more difficulty doing it?

Conley: There are those who will say that you can put in a security standard that doesn't impair the operation. Just the idea of PIN numbers, or personal identification numbers, is an imposition if they have to be changed every week. That is not done. They are not changed every week simply because it is too much of a burden for the people who are operating day in and day out. Yet it would be more effective to do so. You do place a burden directly on the individual customer in the sense that you are requiring him to do something in order to make the transaction. You want to minimize that burden, and yet put in place a sufficient safeguard that he feels secure and also you feel secure that he won't steal all your money. It doesn't slow it down electronically, but it may impose some restriction on the individual that may not be acceptable.

Student: I don't think the stock market would be where it is today in terms of volume levels if it weren't for the ability to move these things around with computers. You just couldn't do it. If you imposed a more stringent security requirement, if you said somebody has to look at this stuff, at some stage you could say that makes sense if, for example, someone has sold half of IBM's outstanding shares and he couldn't possibly have had them.

Student: But that's a much smaller universe of players, recognized brokers, etc.

Conley: I do recall one case where the data was in fact manipulated; I believe there was a firm that was responsible for publishing the information. Someone in the firm was using the data before it was released to the public.

Student: You can reach a certain state, though, where you get so much information that it becomes nearly impossible for human beings to get at it on a real-time basis to find out if something has gone wrong until buildings burn down.

Conley: What you can do at best in those areas is to ensure that the parties who are exchanging the data are authorized to do so. Then you'll have somebody to shoot if there's a problem. Where we really run into a problem is in the area where we don't know who handled or who manipulated the data; in effect, we've allowed unauthorized access by anybody. That is the problem that you want to avoid, where there is no traceability, no audit trail.

Oettinger: I think that opens up another important dimension that ought to be made explicit. You mentioned earlier, in addressing a question on sensitivity, the possibility of someone breaking into the IRS data. This matter of authentication, of finding out who has access to information, or who uses it, is important, because one of the trade-offs is whether to bother protecting or encrypting — and for expensive data, you do — or to leave it alone. With certain kinds of sensitive information, let's say sensitive personnel records, if you don't collect the information in the first place then there's no need to protect it. That's always an option; it's very cheap to protect information that isn't there. That should be kept in mind, so before you get fanatical about protecting something you should ask, "Why do I have it"?

In the middle ground, there is this question of use, and I stress that one because it has great importance, both historically and currently, from a legal point of view. The statutes for telegraphy, as distinct from the statutes for telephony, had historically very few restrictions. Because the telegraphers were inherent in the way telegraphy grew up, telegraphy statutes never said anything against interception. How else could you run a telegraph company without people reading the messages? The penalties in telegraphy are all against illegal use, divulgence, etc., etc., and not against intercepting. Otherwise, you couldn't run the telegraph company.

With the telephone system, the early statutes were the same way, partly because they grew out of the telegraph statutes and partly because you couldn't run a telephone company without an operator. You knew damn well you couldn't have a telephone conversation without the operator overhearing. It's only as you got automatic telephones, when it became feasible to run the system without overhearing, that the notion of wiretap and interception began to be a reasonable thing. But interception of radio waves and interception of telegraphy were not places to protect, because you couldn't. At the same time, in all of these things, there could be penalties for misuse; but the one sure way that you can enforce penalties for misuse of information is if you know who the hell is using it.

So this whole matter of protecting access opens up, among other things, capabilities for introducing a regime of penalties for misuse rather than total protection as through encryption. These notions become very important not only legally, but also technologically, operationally, and economically, and they become a very complicated blend. If you cannot run a telegraph company without telegraphers, it is absurd to write laws that prevent interception. Yes, you might have thought in 1850 or 1870 to encrypt all telegraphy, but you couldn't run a telegraph company using that period's technology for encrypting it; you would have slowed it down to worse than letter mail, and so forth.

If you put all of these things in our contemporary context, you get a sense of the complexity of the problem that Bob is describing and of the shadings of possible approaches to it. You can trade one tool off against another. If you have total control of access, then penalties against misuse become much more thinkable; but if you don't know who's using the system, then protecting it may require something like total encryption, which is expensive.

Conley: Also, we have grown up in two worlds, the communications world and the computer world. I don't know if you noticed that on the chart where I was talking about computer crime (figure 15), not one of the recommendations in there was to protect the communications. And yet, they're talking about a computer system, which includes communications outside of the protected computer complex. In the technical community, those two areas are treated separately. The people in the computer world are developing communications solutions that have been in existence for 20 years. They're starting to develop them now, there are great findings, the writings are coming out — it's fascinating to watch. It's a social problem that we have; the government, because of this growth of the electronic information base, is taking on a broader responsibility, but it's not clear how far the government can or should go.

As you saw up on the chart (figure 14), industry has a large number of computers. They have a lot of data on their own people. The telephone systems that they're installing in industry now can keep track of whom you called and when. What are they going to do with that information? They have it. If you're calling your bookie every day and your employer is watching that data, is that an invasion of your privacy? We don't quite understand all of the ramifications of the information in private communications networks and computer networks. I can go on, and on, and on.

Student: Going back to banks and the stock market, and the question of knowing whom to shoot, do you have any ballpark figure of how much of the banks' transactions are internal, bank-to-bank transactions, and how much are outside people like me going into banks and depositing money into an account or transferring it?

Conley: In the sense of money exchanged, it's probably the same, except that there's just a lot more people like you walking into the banks.

It's not clear what a bank is anymore; I'd like to point that out to you. Sears, for example, will probably be the next biggest bank or stockbroker firm; it's hard to tell at this point. But it looks as if Sears is migrating to become a Merrill Lynch, because you can walk into your Sears store and buy stock. There's no reason why Sears should not become a bank; if a customer banked there as well as doing all the other things, they could give him a debit card instead of a credit card so that as he goes into his account, his transactions immediately come off. We're reaching the point where a bank is no longer brick and mortar.

These institutions are changing. Merrill Lynch went into real estate, not necessarily because they liked real estate, but because a number of major chain stores, with all their existing outlets, are becoming better banks and stockbrokers. There isn't that much money in dealing with the general public, so they'll let that business migrate to someplace else. But they see the major corporations and the major transfers as a different kind of ballgame. They'll still handle the institutional changes to take care of those accounts. You've got to be careful when you talk about banks nowadays, in terms of what they really are and what they do.

Student: In an internal system, you could be reasonably sure of whom you were talking to because of the limited means for communications, as opposed to anybody going up to a machine and sticking in a card that he might have just picked up somewhere. I assume that banks don't run their internal business by inserting cards in machines.

Conley: What you're saying is, the gatekeepers and those on the internal side are the ones who probably are going to violate the system, regardless of how secure it is. That has been the case in the past, and that's probably true, but the ease with which they can violate it is not going to be as great as it used to be. During a normal funds transfer, a bank employee may walk in and look at the code for the day and the customer associated with that code, then walk out and make a phone call and transfer money. When you're dealing at very high levels, you're normally dealing on a personal basis. But if I can imitate your voice, I can transfer money as well.

Oettinger: The old systems weren't models for security.

Student: No, but you never used to be able to steal money from Tokyo.

Oettinger: If you were the wire transfer guy you could.

Student: I mean with the speed and efficiency with which you can do it now. You can do the same things faster.

Conley: There's an international network called SWIFT, the Society for Worldwide Interbank Financial Telecommunications, that transfers funds electronically. It is encrypted, and it is getting a lot of business. Let's take encryption as an interesting example of a solution to protecting some of these transfers. First of all, cryptographic techniques are not exportable to other countries. You don't want to give your cryptographic technique away, because you want to use it to protect your information. It's a delicate area. There are some countries that will not allow you to encrypt to protect anything that would be leaving electronically. You have a lot of international problems that the banking system has to wrestle with. But the only reason I brought in the banking system is that it is a good example of where you can establish the value of both information and security, whether by bank calculation or by government fiat.

Oettinger: I'm delighted with what you have done. Although some of our attention in this course on C^3I tends to be focused on the substance of command and control structures and what is being done for those purposes, evaluating the role and relative value of information is just as important to one's ability to make sound strategic decisions. When you're in the game to outsmart the other guy, be it in a commercial transaction or a military engagement, the question of whether what you're telling yourself or your friends is known to whomever else you're dealing with becomes a very critical element in decision making. The relationship between security matters and command, control, communications, and intelligence seems to me to be fairly self-evident and requires no further bridging to be made.