INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Critical Foundations: Protecting America's Infrastructure
Robert T. Marsh

Guest Presentations, Spring 1999
Charles J. Cunningham, Kawika Daguio, Patrick M. Hughes, Peter H. Daly, Walter Jajko, David J. Kelly, Gregory J. Rattray, Michelle K. Van Cleave, Robert T. Marsh, Randall M. Fort

June 2000

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 1-879716-63-1 **I-00-2**

Critical Foundations: Protecting America's Infrastructures

Robert T. Marsh

General Robert T. Marsh, USAF (Ret.), currently serves as a director and chairman of the board of Comverse Government Systems Corporation, a trustee of The MITRE Corporation, a director of Teknowledge Corporation, and executive director of the Air Force Aid Society. He is also a member of the advisory council of the Georgia Institute of Technology Research Institute. General Marsh was inducted into the Army Air Corps in 1943, and was appointed to West Point in 1945. Many of his assignments during his USAF career were with the Air Force Systems Command (AFSC), where he served as deputy for reconnaissance, strike and electronic warfare in the Aeronautical Systems Division (1969–1973); deputy chief of staff for development plans, Headquarters AFSC, and then deputy chief of staff for systems (1973–1975), and vice commander (1975–1977). From 1977 to 1981, he served as commander of the Electronics Division at Hanscom AFB. His last assignment before he retired from active duty in August 1984 was commander of the AFSC. Since his retirement, he has been employed as an aerospace consultant. He served as the chairman of Thiokol Corporation from 1989 to 1991, and chaired the President's Commission on Critical Infrastructure Protection in 1996 and 1997. General Marsh graduated from West Point in 1949, and holds M.S. degrees in instrumentation and aeronautical engineering from the University of Michigan. Among his many military decorations are the Distinguished Service Medal with two oak leaf clusters, the Legion of Merit, the Air Force Commendation Medal, the Air Force Organizational Excellence Award, and the National Defense Service Medal.

Oettinger: As you know from his biography, General Marsh most recently was the chairman of the President's Commission on Critical Infrastructure Protection (PCCIP). It's a pleasure to introduce him as an alumnus of this seminar. I was looking back at when he was last here, which was in 1982, the first year in which he was the commander of the Air Force Systems Command. At that time, he spoke on "Air Force C^3I Systems." Just to give you a sense of how the world has changed, the other speakers included a man named Richard Ellis, who at that time was CINCSAC, commander in chief of Strategic Air Command, and his topic was "Strategic Connectivity." It was still the height of the Cold War, and there was great concern over maintaining communication among the elements of command and control over strategic nuclear forces. A man named William Miller spoke on "Foreign Affairs, Diplomacy and Intelligence." He was a former ambassador to Iran, and his theme was how screwed up things were when we failed to see all the signals of the demise of the Shah. So the world marches on.

It is a pleasure to welcome Tom Marsh in his modern, contemporary, PCCIP capacity. He has assured me that he is willing, yea eager, to be interrupted with questions anywhere along the line, so please feel free to go at him. So saying, I turn it over to him. Thanks so much, Tom, for joining us again.

Marsh: Thanks, Tony, for having me here. I'll stand and sit and do various things. I really am pleased to talk with you all because I think it's very topical, the protection of the life support systems of the nation—and that's how I view our so-called critical infrastructures. It's something that we're all very concerned about these days. I think you need to be and probably are. I'll walk you through what the commission was all about, and how we went about our work. I'll do that rather quickly, and then summarize our key findings. Finally toward the end, I'll get into "So what?"—what's being done about it.

We were given a pretty daunting task by the President. It was to look at the critical infrastructures; define their vulnerabilities; try, as best as we possibly could with all the resources of the intelligence community, to identify the threat to these critical infrastructures; and then develop a strategy and an implementation plan on how we could assure their protection (figure 1). It was a very tough task.

Recommend a national policy for protecting and assuring *critical national infrastructures*

- Determine vulnerabilities
- Identify threats
- Develop policy and legislative issues
- Develop policy recommendations and implementation plan

Figure 1
Mission

These were the critical infrastructures that were specified (figure 2). You can readily identify them. I might say a word about government services. It doesn't mean how to assure the continuity of leadership of the country, although sometimes it is meant as that. It means assuring that government services provided to the society are running smoothly. They include Social Security, Medicare, et cetera—those kinds of services—and emergency services such as 911 as well.

- **Telecommunications**
- **Electric power**
- **Transportation**
- **Oil and gas delivery and storage**
- **Banking and finance**
- **Water**
- **Emergency services**
- **Government services**

Figure 2
Critical Infrastuctures

To set the stage for thinking about this problem, an interagency working group had been set up prior to the formation of the commission. They observed many of these happenings all over the nation (figure 3). As you well know, some were perpetrated by terrorists, some by forces of nature, et cetera. There had been a major power outage that affected many states in the western region of the United States for an extended period; 911 systems had been spammed down; we had lost our air traffic control system a number of times in major areas; and so on.

What worried the interagency group was: What do you do about things like this (figure 4)? Whom do you call? What do you need to know about these outages? How quickly can you determine the cause? Is it just a coincidence? Is it a natural occurrence, or is it possible that it's planned? Can you respond, and if so, how? That set the stage for the kind of problems that we were to address.

There was also the recognition (I know you've thought about it, and it's perfectly obvious) that almost overnight we have become vitally dependent upon these information technology-embedded critical infrastructures, and yet we take them for granted (figure 5). When you pick up the phone, you expect to get a dial tone. When you turn the faucet on, you expect pure water to flow. When you dial 911, you want and expect emergency response. That dependence is part of our social fabric.

There's also increasing interdependence here, and I don't want to get into it. That's a whole topic unto itself. I know you've discussed it somewhat in this class. The electric power industry depends upon the Global Positioning System (GPS) and on telecommunications, and, of course, vice versa. Even emergency backup systems for more than, say, six hours of operation depend upon the transportation system to replenish fuel supplies, et cetera. There's increasing interdependence among all systems. We need to understand it better; today it's not well understood. Finally, there's no question—you see evidence of it every day—that there's increasing vulnerability in these systems as they incorporate more and more of this wondrous information technology.

I probably don't need to tell you this, but the world has changed in all of these respects

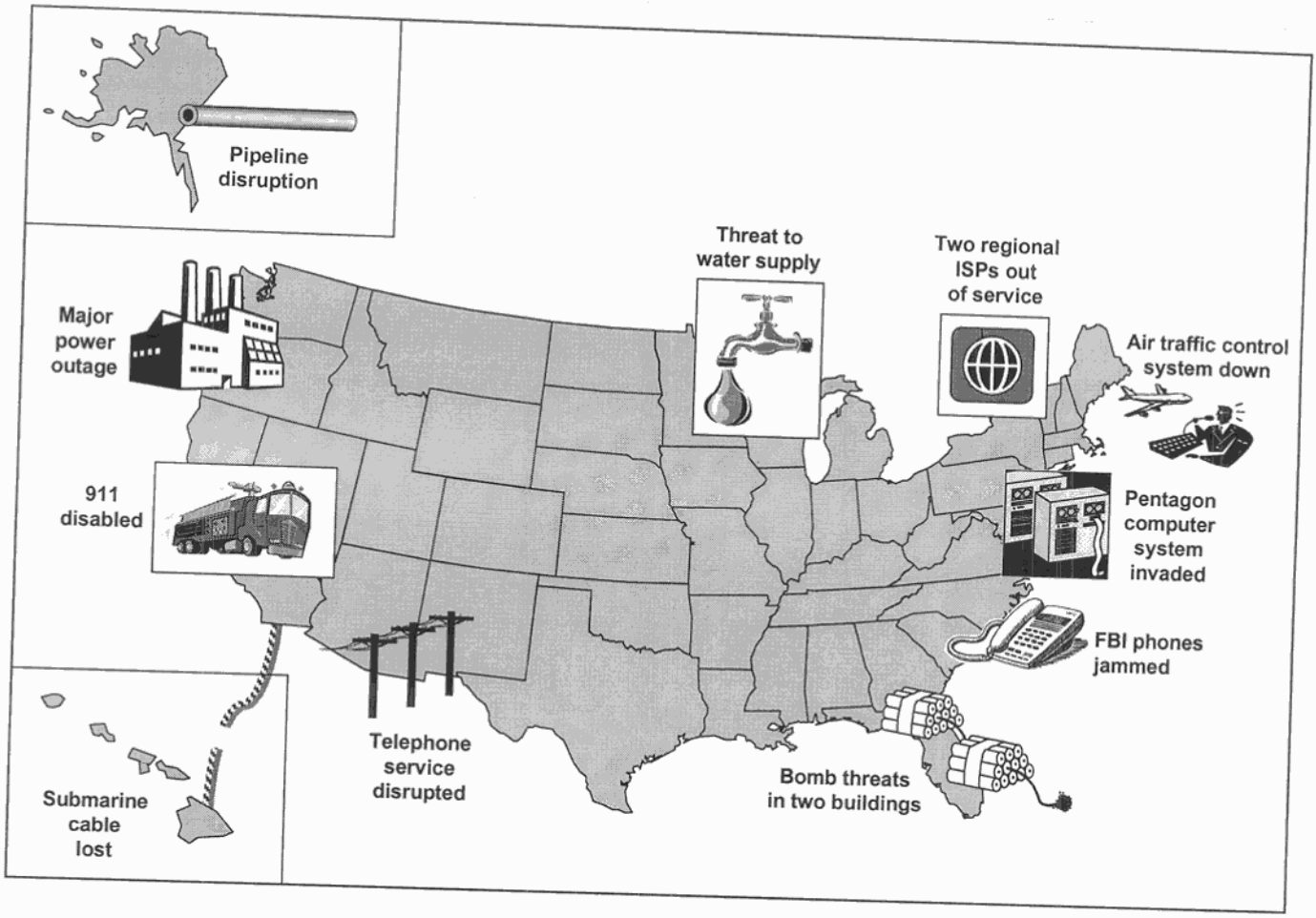

Figure 3

Imagine...

(figure 6). As we enter the new millennium, which is so information-technology based, we must come to grips with how we assure ourselves of the availability of critical services even in the face of determined efforts to deny us those capabilities.

- Whom do you call?
- What do you need to know?
- How quickly?
- Why?
- Is it a coincidence?
- Can you respond?

Figure 4

What Do You Do?

I don't want to belabor interdependency at this point, but we found that all of the critical infrastructures are critically interdependent (figure 7). As we looked at disaster plans within a given infrastructure, we found that they took very little account of the assurance of the other infrastructures upon which that infrastructure depends. That is, the electric power people really didn't concern

- Increasing dependence
- Increasing interdependence
- Increasing vulnerability

Figure 5

Why the Commission?

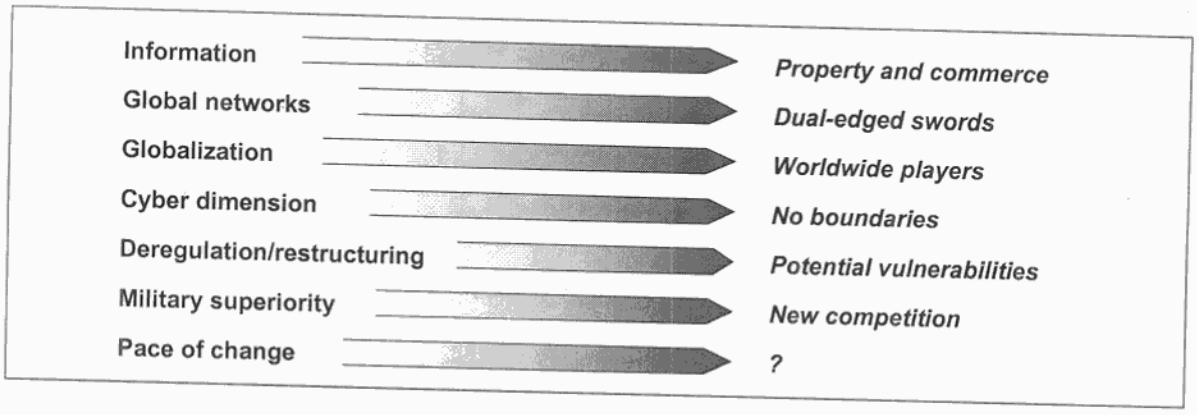

Figure 6
The World Has Changed

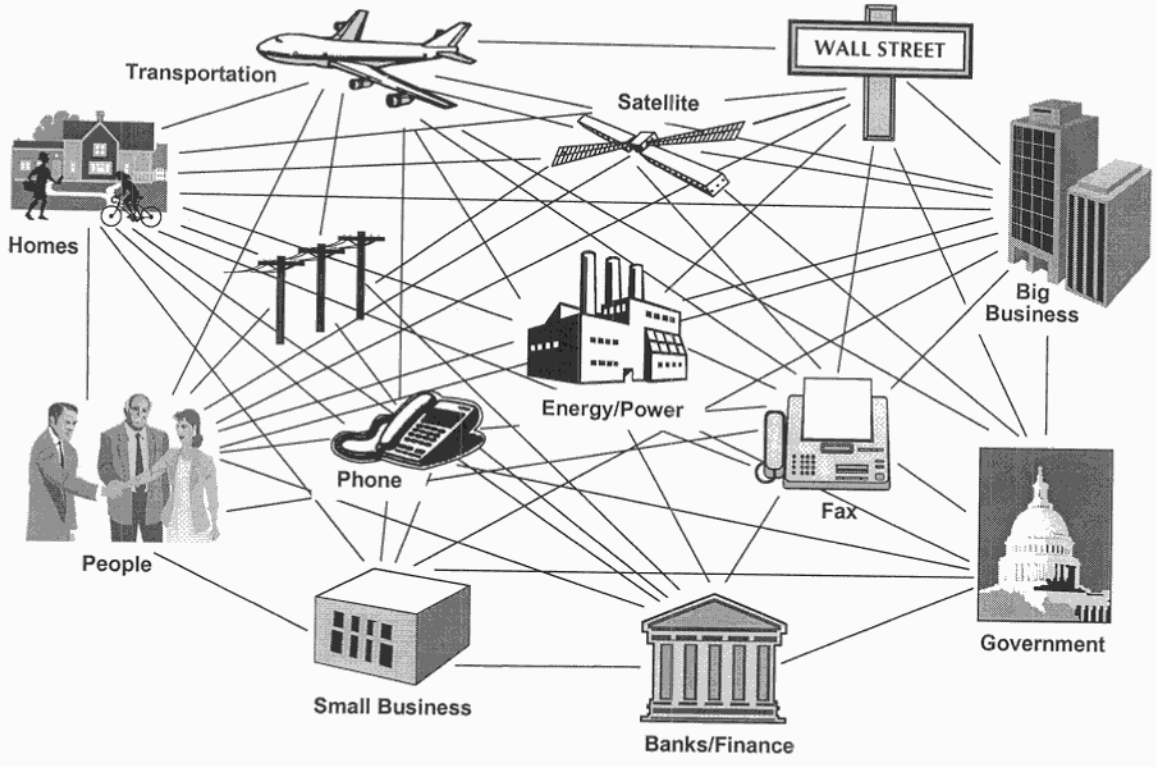

Figure 7
Interdependency: Ill Defined—Not Well Understood

themselves with what would happen if the telecommunications, or the GPS signal, or the fuel supplies, or the transportation services, should be denied. They had conducted their own stovepipe type of vulnerability analysis, but not the interdependency type of analysis that's really required.

Why would anybody want to harm our infrastructures (figure 8)? Obviously, with respect to national security, to reduce our ability to act in our own national defense interest, and there are those who would like to see confidence in the public services the government provides be eroded, resulting in a lowering of morale. Finally, many recognize that it's the stability and assurance of these critical infrastructures that is the base of our great economic strength. A company can move out to Podunk and be assured of good water, good telecommunications, and good electric power. That's not assured in many countries of the world, but it is here. Undermining confidence in our infrastructures would seriously undermine our economy.

Oettinger: What would a parallel picture look like, that asks, "Why *not* attack infrastructures?" Let me give you what motivates the question. In Cold War terms, for example, there were good reasons why folks agreed to treaties that said they would not touch each others' national technical means of verification. They recognized that stability, on the one hand, or, if a conflict got started, some reasonable (short of mutual assured destruction) war termination scenario, on the other hand, required some minimal communications infrastructure. So oddly enough, at the height of the Cold War, there were certain things that the antagonists agreed shouldn't be touched because of a variety of reasons. Did your commission think about that?

Marsh: We thought about that somewhat. If you have the umbrella of the nuclear threat, then preservation of infrastructures takes on increasing importance for such purposes as termination, et cetera. But if you're thinking in terms of the great strength of this country, it's our military strength. Hence, how can you do serious damage to this nation without a battlefield confrontation? We believe that in the future adversaries will look to the infrastructures as asymmetrical, very attractive targets that they can seriously damage and yet not have to confront weapon to weapon. I agree that there certainly are scenarios that say, "Don't destroy the enemy's infrastructures."

Just to think a little, back in World War II, attacking this nation's infrastructures would have been a mammoth undertaking. An enemy would have had to invade us or mount an aerial attack, a capability no country had at that time (figure 9). It would have been a very costly operation. In the Cold War period, bombs and missile capabilities began to threaten our infrastructures in the United States. But even then, we knew who posed the threat; we devised means to alert ourselves to it and deal with it reasonably effectively, and deter it. But now the cost of such a capability is zilch. All you need is a computer, some basic skills, and the tools that are readily available, even on the Internet, to do serious harm. Such capability is ubiquitous in this world today. So, times have really changed.

Here's what our commission structure looked like (figure 10). It was very interesting. We were a full-time commission (not many are); that is, everybody worked full time on the commission. We were half from the private sector and half from government. The government half were senior executives from all the involved agencies of government; SESs (members of the Senior Executive Service) in all cases. In the case of the private sector, we recruited people from AT&T, from Pacific Gas and Electric, from the Federal Reserve, et cetera, to come in and serve full time on the commission. They were generally up-and-comers in their industry, people their CEOs recommended. Incidentally, it was quite a hassle getting them on board quickly and in the full employ of government. They had to put up with a lot of red tape they didn't like.

We pulled that together pretty quickly. We had a steering committee composed of [National Security Advisor] Sandy Berger, [Deputy Attorney General] Jamie Gorelick, and [Deputy Secretary of Defense] John

White, and others. We had an advisory committee co-chaired by Senator Sam Nunn [D-GA] and Jamie Gorelick, after she left the Justice Department, and CEOs from many of the infrastructure companies—utilities, bankers, and so on—who advised us and reviewed our efforts.

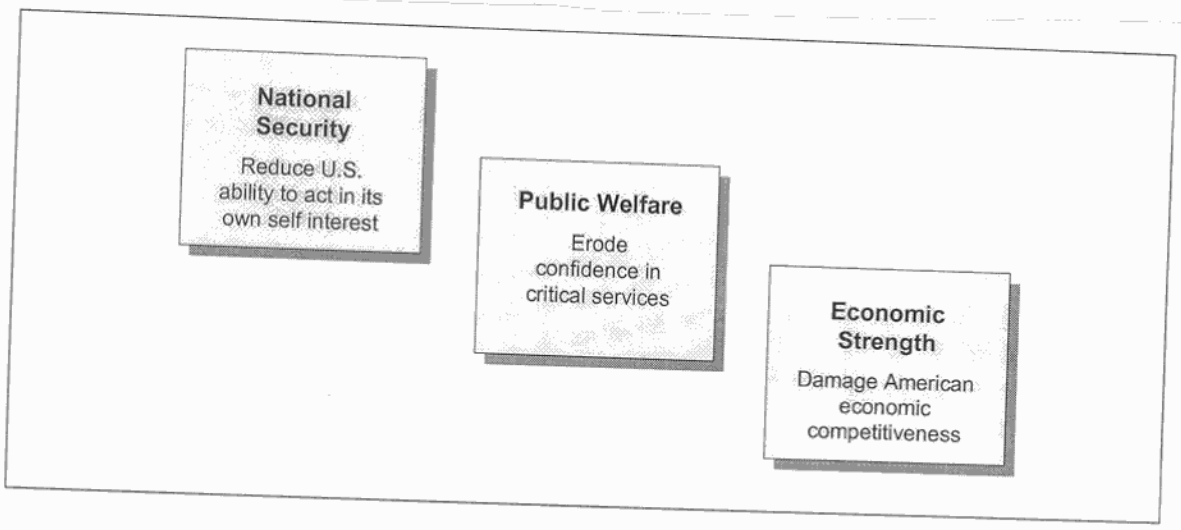

Figure 8

Why Attack Infrastructures?

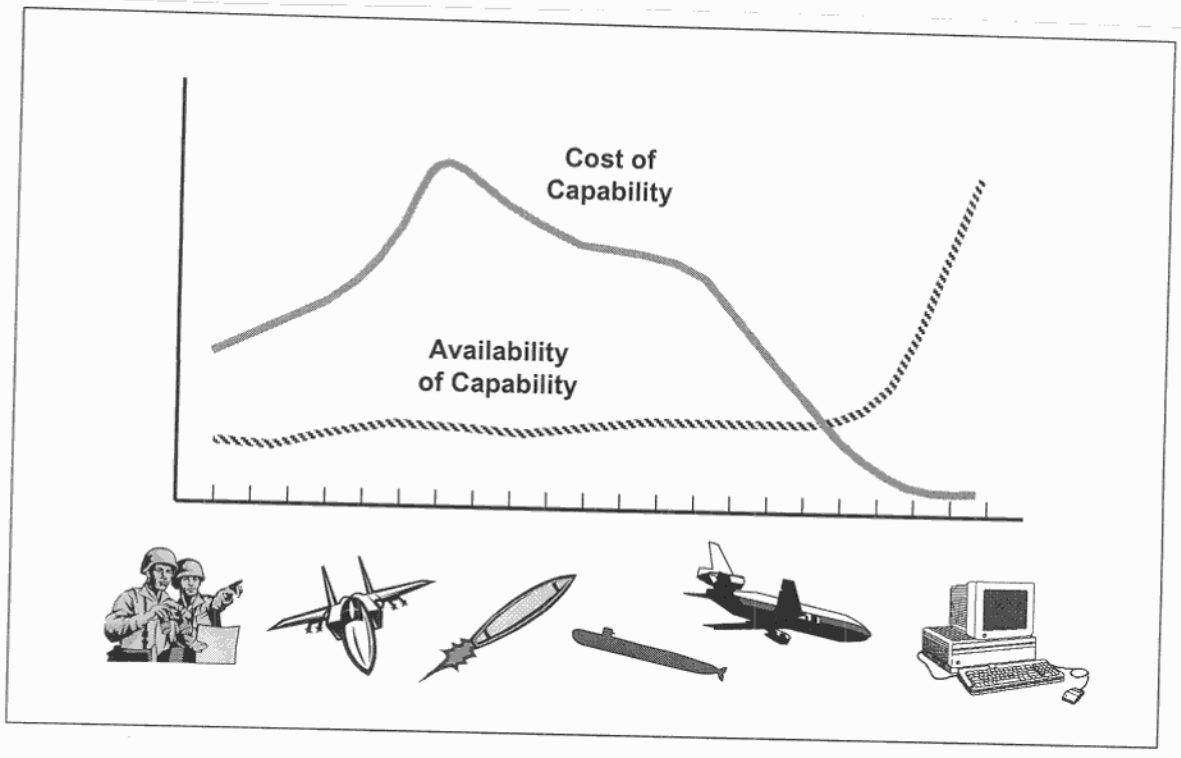

Figure 9

Evolution of Threat

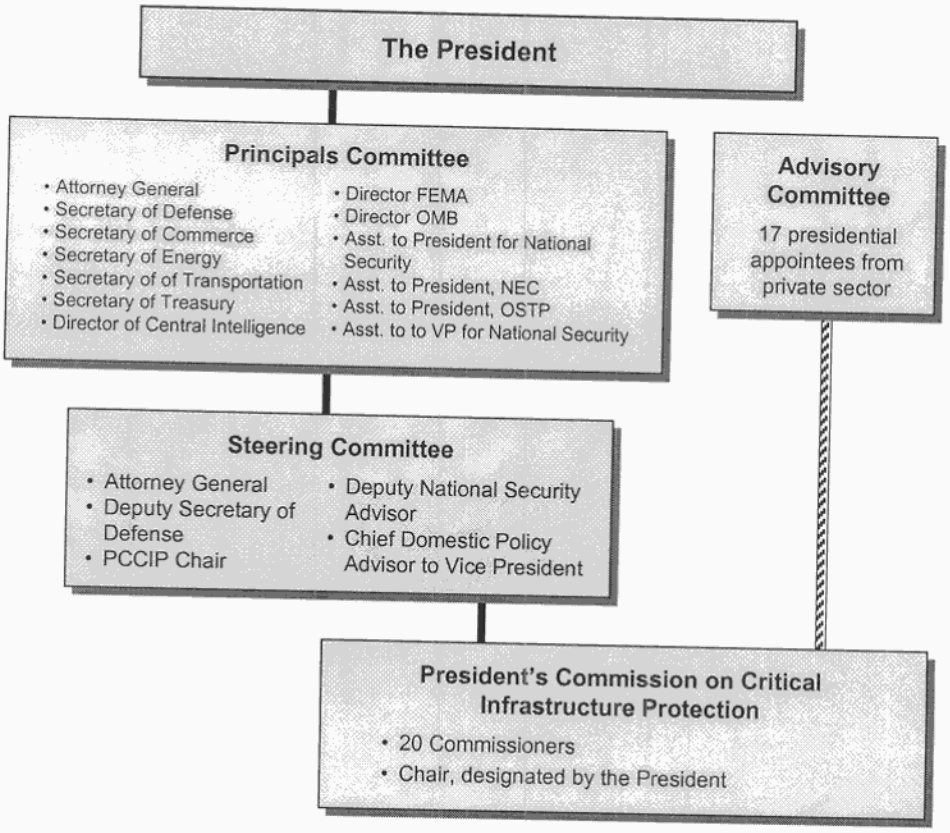

Figure 10

Report Review

Student: What's the actual role of Richard Clarke, about whom the *New York Times* reported a couple of weeks ago as the man who protects America, or as the czar, or technocrat, or "intellocrat?" Nobody else in the White House actually knows what he's doing, but in the daily business he handles everything of that type. It seems to be a dual structure.

Marsh: If you'd hold that, and let me talk about what we recommended, and then the role that Clarke was put in as one of our recommendations, I'll be happy to discuss it. I think it will fit in better a little later.

We held a series of public meetings around the country, soliciting comments on our work. We put material out in advance (figure 11). We held a number of conferences around the country, a number of simulations—wargames, if you will—and made lots of individual contacts. It was a wide-ranging effort. We spent six months characterizing the infrastructures. What do you mean when you say "America's electric power industry"? Nobody has put that down on paper. What are the critical nodes? What are the vulnerabilities? What is the telecommunications industry? What is the water supply industry in the United States? and so on. We spent six months divided into teams devoting full time to answering those questions. The result is a wonderful database today.

I'll say a few words about the threat (figure 12). First, a National Intelligence Estimate was conducted in harmony with our effort. I can't say much about that except the bottom-line conclusion is that a threat of the nature we've been describing is sure to develop in time. So, rather than look for that smoking keyboard (we didn't find one; that is, we know of nobody who has a firm plan to launch a disabling attack on the nation's

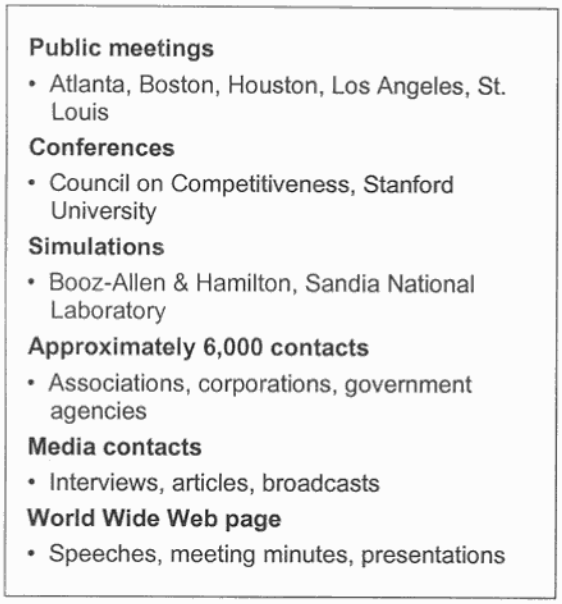

Figure 11
Outreach Efforts

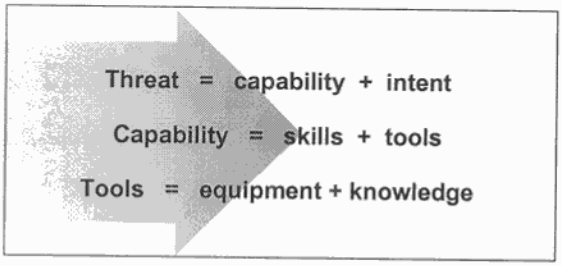

Figure 12
Threat

critical infrastructures), what we did instead was to say that the threat really consists of capability plus intent to do harm, and capability equals skills and tools. We concluded that it's a capability that most young teenagers today have, and that all of us can find tools that are readily available on the Internet. So all it takes is intent to do harm, and there are lots of people, lots of entities, that would like to do us harm.

Here is the arsenal of tools (figure 13). They're all of these. We're particularly concerned with denial of service, not these annoying little hacker attacks, but true denial of services that we have become increasingly dependent upon. We're concerned about Trojan Horses: implanting devices in a carefully laid plan to cause disruption in lots of key areas. We're also concerned about data modification. Naturally we're concerned about all of the items on this list, but those were ones that received special attention.

This is simply to highlight the importance of the insider (figure 14). As you know, the threat spectrum ranges from the hacker, who gets a thrill out of breaking into somebody else's computer, to the information warrior, who has the intent of doing serious harm to a nation. No matter what you do in terms of putting good security in place, all may be to no avail against an insider, whether he be suborned by somebody who wants to do serious harm, or acts on his own aggrieved behalf. The insider poses a tough problem, and we spent a lot of time exploring how to deal with that problem. We can talk more about that later.

I don't want to stress vulnerabilities too much (figure 15). We can talk about this a long time. Generally, people know what our physical vulnerabilities are. They probably don't know what the key nodes are, or what are the most vulnerable nodes within critical infrastructures. We did a lot of work to identify those. There's no question, though, that cyber vulnerabilities exist in spades and are growing.

There's also little appreciation for interdependency. What bothers us is that much vulnerability information is readily available. Incidentally, our detailed volumes on vulnerabilities of the critical infrastructures are classified. We classified them because we concluded that a compendium of all of this information (even though unclassified, and nearly all of it is) would provide a road map to those intent on harm. That classification is being reviewed today. We recommended that the U.S. Security Policy Board explore how the nation could protect this critical vulnerability information. That is, it need not be military Secret or Top Secret, but how could vulnerability information on our critical infrastructures be protected from general, wide distribution?

In a general sense, we found that the vulnerabilities are serious, and increasing (figure 16). We found everywhere that what industry needs is a better appreciation of the problem

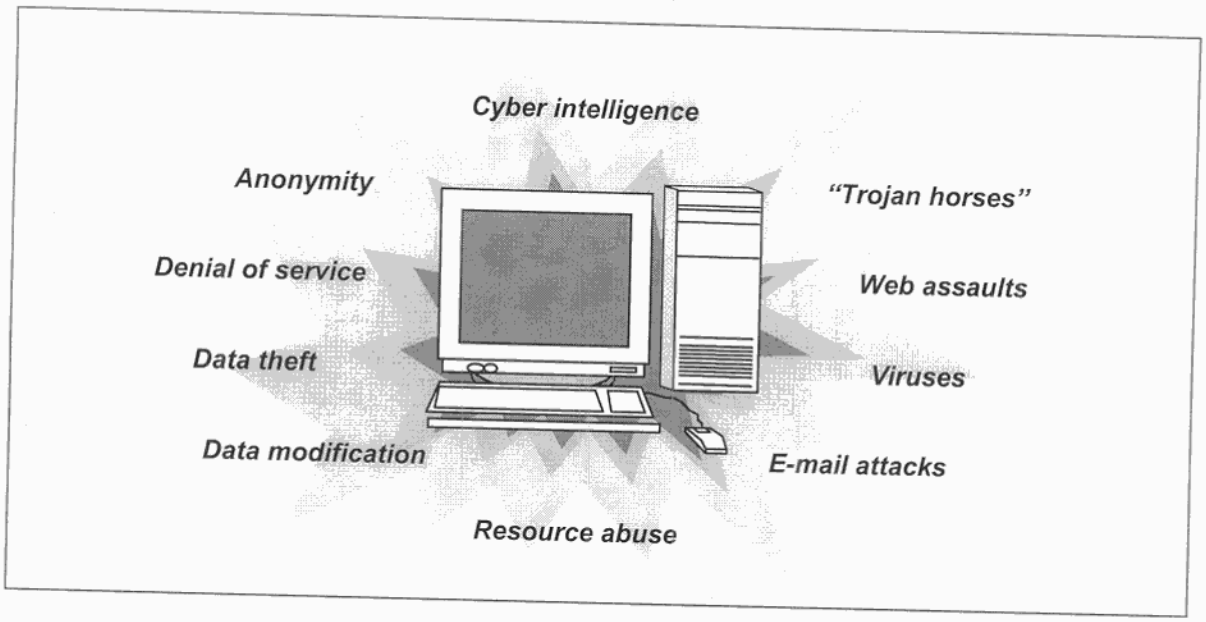

Figure 13

A New Arsenal

National Security Threats	**Info warrior**	**INSIDERS**	Reduce U.S. decision space, strategic advantage; create chaos, target damage
	National intelligence		Information for political, military, economic advantage
Shared Threats	**Terrorists**		Visibility, publicity, chaos, political change
	Industrial espionage		Competitive advantage, intimidation
	Organized crime		Revenge, retribution, financial gain, institutional change
Local Threats	**Institutional hacker**		Monetary gain, thrill, challenge, prestige
	Recreational hacker		Thrill, challenge

Figure 14

Threat Spectrum

and a better sharing of government information on the threats. As the government's systems are penetrated, and it learns how to deal with it using better firewalls, et cetera, that information should be shared with the private sector. We felt that the federal government has a very important role to play. National awareness is key. We must raise awareness throughout the nation.

When I say responsibility is shared, you must open your mind to this. These critical infrastructures are vital to our national defense, and if we are engaged in a serious confrontation with another country, then the private sector—owners and operators of these critical infrastructures—is really on the front line. So, for the first time, the private sector is a member of the national defense team.

- **Physical vulnerabilities known**
- **Cyber vulnerabilities growing—constantly changing**
- **Little appreciation for the interdependencies and complexities**
- **Vulnerability information readily available**

Figure 15
Vulnerabilities

- **Vulnerabilities are serious and increasing.**
- **Information sharing is the most immediate need.**
- **The federal government has an important role in the new alliance.**
- **National awareness must be elevated.**
- **Responsibility is shared between the public and private sectors.**
- **The legal framework needs modernization.**
- **R&D and investment are not sufficient.**
- **Government needs to organize itself better.**

Figure 16
Findings

There's a shared responsibility for their protection. I haven't framed that quite as well as I should, but that's what I'm getting at.

No place in the statutes do you find the word "cyber," so the legal framework has to be updated. We made recommendations in a number of areas (I'll point those out a little later) to deal with that.

There's no question that the R&D investment for infrastructure protection, both in the public sector and the private sector, is inadequate. I'll discuss that more. Also, the government needs to organize itself to address this problem. I'll be specific about that.

The important point is that it's a shared risk. This is not something for government alone to solve. It has to be addressed by both the public and the private sector. Getting private sector buy-in is the real challenge, because they do not perceive this to be a serious problem today. We must raise that awareness (figure 17).

- **Achieve private sector buy-in**

- *Shared ownership of the problem*
- *Joint solutions required*

Figure 17
Most Significant Challenge

In a nutshell, what the private sector must do is protect itself against the tools and report attacks (figure 18). The federal government has to collect and disseminate information about tools, develop information about the threats, and issue warnings. It also must take the lead in developing tools and techniques to deal with the threat.

When we say the private sector should protect itself against the tools, generally speaking (this isn't 100 percent), the same tools would be employed by a recreational hacker as by the information warrior of a foreign state. If the private sector protects itself against the recreational hacker and the petty thief, it is taking an important step toward protecting against a nation-state attack. So that's why it's a shared responsibility. If the private sector takes prudent steps to protect itself against conventional threats that any business faces, then it will be going a long way toward protecting the nation against those who would do serious harm.

Student: Yes, but I think for the private sector it's a little bit different. There is a difference between hacker attacks and state-supported attacks because, for example, hacker attacks are usually dealt with from a cost/benefit perspective. For example, it is possible to install safeguards against cloning of smartcards and things like that, but most banks consider it a matter of course, so they prefer to compensate people who lose money by others' fraud and so on rather than install security measures. So, is the American government trying to explain the difference to the private sector between the grave conse-

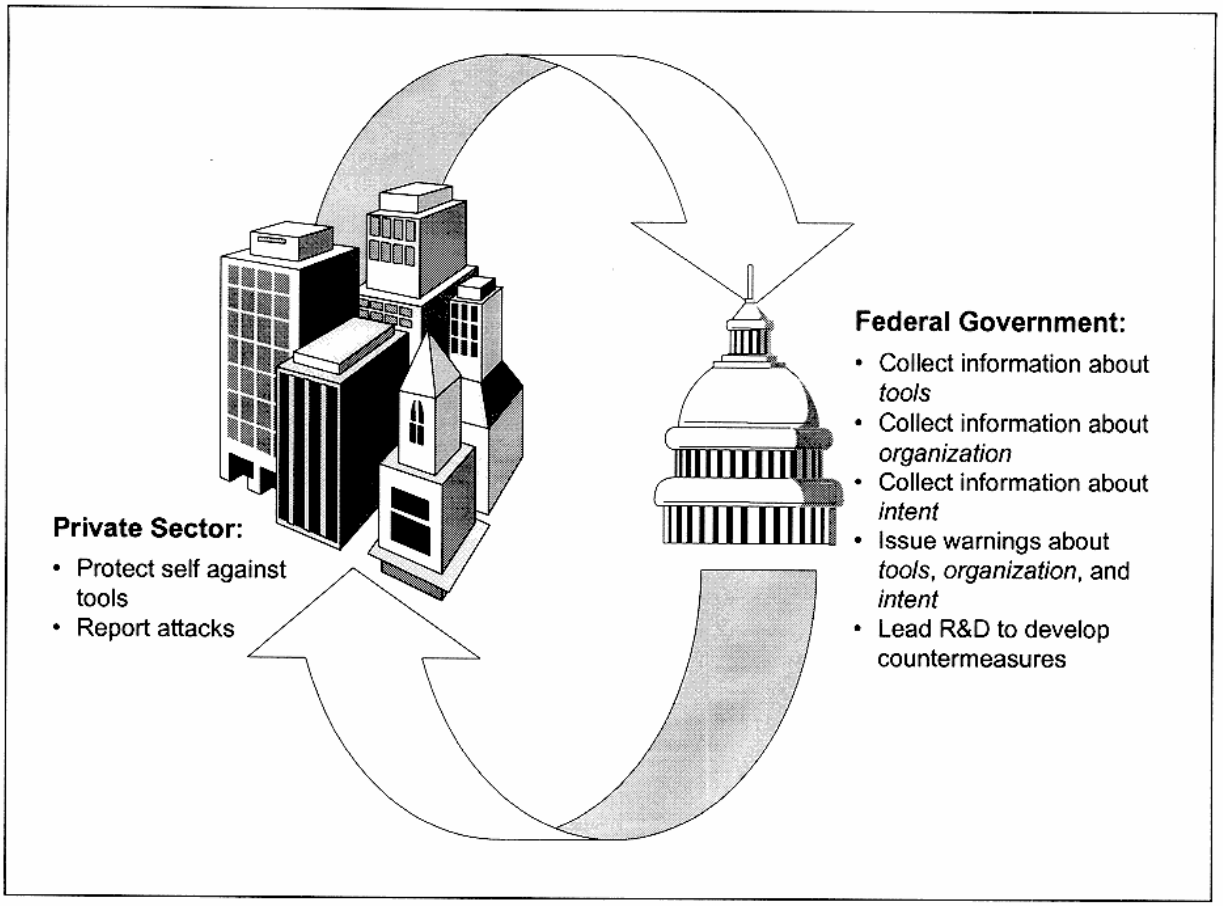

Figure 18
Responsibilities

quences of organized attack by some state versus a hacker attack? How does the state try to communicate to the private sector?

Marsh: I'll go through those recommendations, but you're right on. It's a government responsibility, in this instance, to share information with the private sector to raise their awareness. We believe that if the private sector is properly informed of the threat, just based upon their business interests, they'll be motivated to take the steps to provide the necessary protection. I'll develop that a little further as we go.

Now, this isn't to say that there are not today, and may not be, some kinds of attacks against our infrastructures that in intensity and gravity are above and beyond what you'd expect a prudent businessman to protect against. If those arise, then it does raise a question: Does the government have to incentivize the private sector and, perhaps, provide tax relief for those above-and-beyond defenses that might be necessary? First, to this point we haven't identified those threats. Second, I don't think you'd need to worry about those more extreme cases until you've raised the level of awareness and protection up to a pretty substantial level already. I think those are pretty obvious (figure 19).

I just can't say enough about this (figure 20). Government and private industry aren't in partnership. Most times they're at odds and have opposing interests. But we really mean this: We must form, in an unprecedented way, a new partnership to jointly protect our assets, government and private sector, in our common interest, against those that would do harm to them. So, that's a hallmark of our effort.

What our recommendations really come down to are those that involve better sharing

- **Government must lead by example.**
- **Start with owners and operators.**
- **Build on that which exists.**
- **Promote voluntary cooperation.**
- **Maintain existing oversight and regulation.**
- **Practice continuous improvement.**

Figure 19
Guiding Principles

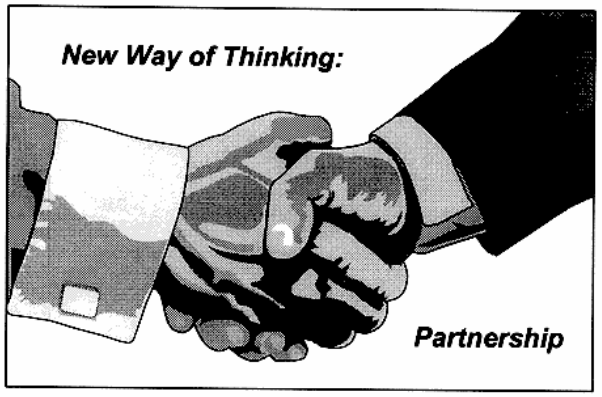

Figure 20
Fundamental Observation

of information, the actions the government ought to take, a number aimed at education and awareness, and a number of the government getting its own house in order (figure 21). The government can't exhort the private sector to raise the protection level of its systems when its own are under constant attack and as obviously vulnerable as they are. There are a number of legal initiatives that we recommended, quite a bit on R&D, and, finally, recommendations of how to structure this partnership that's needed.

These are some of the government actions mentioned in the previous slide (figure 22). NIST (National Institute of Standards and Technology) and NSA (National Security Agency) are deeply involved in this, as you all know. NIST and NSA should offer their expertise to the private sector in an unprecedented way, a way they're not used to. We've made some specific recommendations in that regard. They and DOD need to help

Goals:
- **Improve conditions**
- **Establish infrastructure assurance roles**
- **Foster partnerships**
- **Coordinate global interests**

- Information sharing
- Education and awareness
- R&D
- Legal initiatives
- Government actions
- Leading by example
- Structuring the partnership

Figure 21
Recommendations

Objective: Properly prepared owners and operators and state and local governments to accomplish their infrastructure protection roles

---

- NIST and NSA offer expertise to encourage development and adoption of security standards.
- NSA, DOE, and DOD perform vulnerability risk assessments.
- Encourage industry to develop risk methodologies.
- Federal government review sensitive owner and operator information prior to publication.
- Double Nunn-Lugar-Domenici funding.

Figure 22
Government Actions

the private sector perform vulnerability analyses. Many of you refer to that in simple terms as Red Teaming. We do it to our own government systems. We need to do that to the private sector to open their eyes. There are some legal impediments that must be dealt with. They must do better risk assessment. Certain elements of the government were putting on the Internet much vulnerability information about the infrastructures. That must stop. I'll get specific on that if anybody is interested. Finally, we want the Nunn-

Lugar-Domenici program against terrorism[1] to cover cyber terrorism. We made a recommendation in that area.

The private sector is always reluctant to share information with the government (figure 23). Their concerns are, "Before I do it, you must assure me you're going to protect my proprietary information. If I ask for anonymity ..." (like a bank reporting "I've been intruded, and here's how they did it," et cetera) "... you'd better not use my name. Don't come back after I exchange protection information with another bank and get me on antitrust. You must ease that."

Objective: Free interchange of essential threat and vulnerability information among all parties—public and private

- Protect proprietary information.
- Provide anonymity, as needed.
- Ease antitrust concerns.
- Organize sector "clearinghouses."
- Establish public-private Information Sharing and Analysis Centers.

Figure 23

Information Sharing

We can't deal with each and every company out there, every electric power company, and the rest, so we recommended—and this is central—that the industries develop clearinghouses where they, through their associations or other means, would encourage the free exchange of information on cyber attacks, cyber fixes, and best practices. Those clearinghouses would exchange information of the same nature with the federal government. If the companies insisted on anonymity, the government would respect it. If, on the other hand, they needed law enforcement assistance, they'd get that immediately. Proprietary information would be protected.

Our goal was for one clearinghouse or a number of them to be formed and become what we call Information Sharing and Analysis Centers (ISACs), places where information could be collated and correlated. "There's been an unauthorized intrusion over here that resulted in *this*; another one over here; and here was the nature of it." The ISACs need to bring that information together, try to understand what's going on, get better situation awareness of what's happening, and then disseminate information out to others to facilitate taking corrective action. We think that's essential. Information sharing and analysis functions must be performed in the private sector, not in the federal government. The private sector is reluctant to share that kind of information with the federal government, so the federal government has to promote ISACs and assist in getting them established in the private sector.

We want the bully pulpit power of the White House to be used for education and awareness (figure 24). We must raise the level throughout society. Kids have to understand that it's trespassing when you go into somebody else's computer. You wouldn't open the door of your neighbor's home and go into the house uninvited. It's the same if you go into somebody else's computer. We

Objective: Heightened awareness of critical infrastructure threats and vulnerabilities

- Conduct White House conferences on computer ethics.
- Conduct national awareness campaign.
- Establish simulations and round tables.
- National Science Foundation fund network security graduate programs.
- Establish partnership among NIST, NSA, Department of Education, and industry to develop programs for education and training of information assurance specialists.

Figure 24

Education and Awareness

[1] The so-called Nunn-Lugar-Domenici legislation, the Defense Against Weapons of Mass Destruction Act, constitutes Title XIV of Public Law 104-201, the National Defense Authorization Act for Fiscal Year 1997. It charges agencies of the federal government with putting systems into place to protect the public against terrorists.

must raise that ethical standard. We recommended that the National Science Foundation make grants, both to promote network security education at the graduate level, and to develop graduate faculty for this new discipline.

Finally, system administrators are key in this business: those people who control access to their systems. They make sure that nobody gets in and amends the operating system except those with authority. System administration is an area that really needs to be elevated in importance and training in order to make our systems more secure.

I don't need to say much more about leading by example (figure 25). The government must clean up its act in this area. We can't tolerate news releases every day about

Objective: Federal government systems and processes serve as "benchmarks" for infrastructure assurance

- Use best practices and set standards.
- Conduct certification.
- Conduct information security pilot programs.
- Formalize intelligence priorities.
- Acquire and retain cyber-qualified law enforcement personnel.
- Emphasize security in national airspace design.
- Address GPS vulnerability.

Figure 25
Leading by Example

cyber break-ins and screwing up this or another system. It puts the government at a disadvantage in talking the private sector into getting its act together if its own systems are so vulnerable.

Some major federal legislation needs review and amending. The Stafford Act, which governs the Federal Emergency Management Agency (FEMA) and assistance for recovery from disasters (figure 26), doesn't address cyber disasters at all, but should. The Defense Production Act is a source of funding for unique R&D and production needs, for instance, detecting unauthorized intrusions, assessing the situation, and simulating interdependencies.[2]

Objectives:
- **Increased effectiveness of federal assurance and protection efforts**
- **Enhanced private sector ability to take protective action**
- **Impediments to partnership assessed**

- Major federal regulation
- Criminal law and procedure
- Employer-employee relationship
- Legal impediments to information sharing

Figure 26
Legal Initiatives

Most cyber crimes today are considered misdemeanors, but they ought to be treated in a more serious way. We made recommendations that the federal sentencing guidelines be revised so that the true implications—that is, the damage done by unauthorized intrusions—be the basis for sentencing.

Regarding the employer/employee relationship, we found that in many states you can't inquire into a person's criminal record as a prerequisite to hiring. It's our feeling that for such key slots as system administrator of a critical infrastructure, you should be able to check the trustworthiness of individuals before you hire them. Consequently, we made recommendations in that regard. Finally, there's a long list of legal impediments: proprietary rights, antitrust, the Freedom of Information Act, et cetera. They all come under that last heading, and we had a lot to say in that area.

[2] The Robert T. Stafford Disaster Relief Act of 1984, amended in 1988, gives FEMA authority over military forces in a state of emergency. The Defense Production Act of 1950 charges the Commerce Department with identifying critical defense-related industries, assessing their ability to meet peacetime and national security needs, identifying constraints on production, and proposing remedial actions.

Now, according to our estimate, the federal government is spending about $250 million a year on information assurance (figure 27). Most of that is NSA funding for crypto-type work. Very little is going to the purposes of detection, warning, anti-intrusion, trace-back, et cetera. We recommended growing that over a five-year period to approximately $1 billion a year. The federal government spends about $70 billion a year on R&D. As we become an information technology-intensive society in the next millennium, we should devote on the order of 5 to 7 percent of that federal funding to the protection of our critical systems. Incidentally, all agencies combined are bidding for more than that; it's not nearly as large as it sounds.

What should the federal government do to get its act together (figure 28)? We made these recommendations. We recommended an Office of National Infrastructure Assurance in the White House; it should have high visibility and these roles. We recommended a National Information Assurance Council, appointed by the President, composed of prominent CEOs from the infrastructure sectors and selected cabinet members, to propose policy to the President regarding this shared problem of both the public and the private sector. There should be an office to support both the council and the White House office, all that at the policy level.

At the operating level, we recommended that each industry sector appoint a coordinator to deal with the federal government to promote these clearinghouse functions. We recommended that each federal agency designate a person to work with the coordinators to facilitate and promote development of the clearinghouses. We recommended that the ISAC, or ISACs, be established with the support of the federal government, as was done with SEMATECH or similar enterprises. It could be along the lines of the Centers for Disease Control, where they've broken the barrier between the physician and the center for collection of information. They've created a trusted environment where the privacy of the patient is not violated, and yet essential information flows. Finally, we recommended that a national warning center, the National Infrastructure Protection Center, be set up within the FBI. That's been done.

Those were our recommendations for the national structure (figure 29). It looks a little bit like this (figure 30).

So, what are the next steps? You are probably familiar with PDD 63, the presidential directive that essentially said: "Move out on this." It is unique in that it directs the implementation of all our recommendations. Not a single one was left out. It designated Dick Clarke as the national coordinator. Now, Dick Clarke is a wonderful man, but

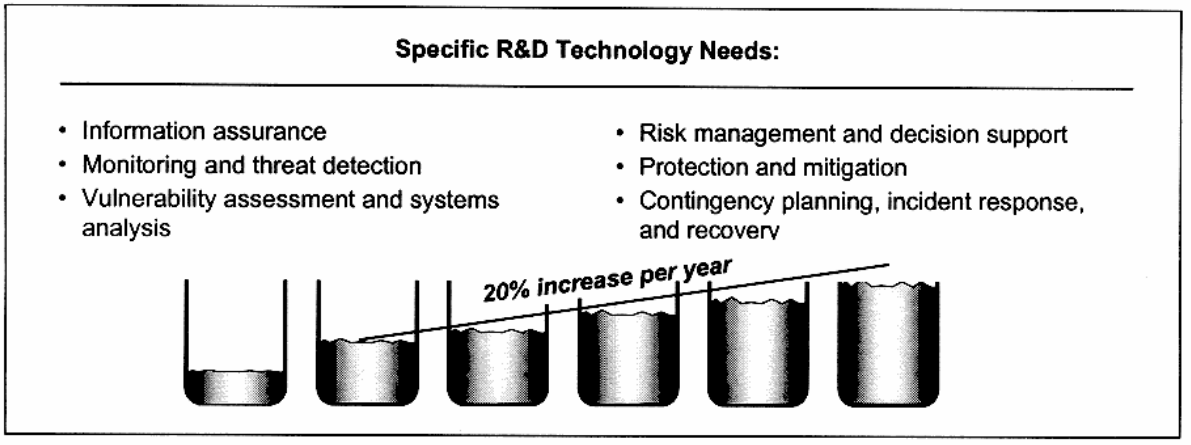

Figure 27
Recommendations: Research and Development

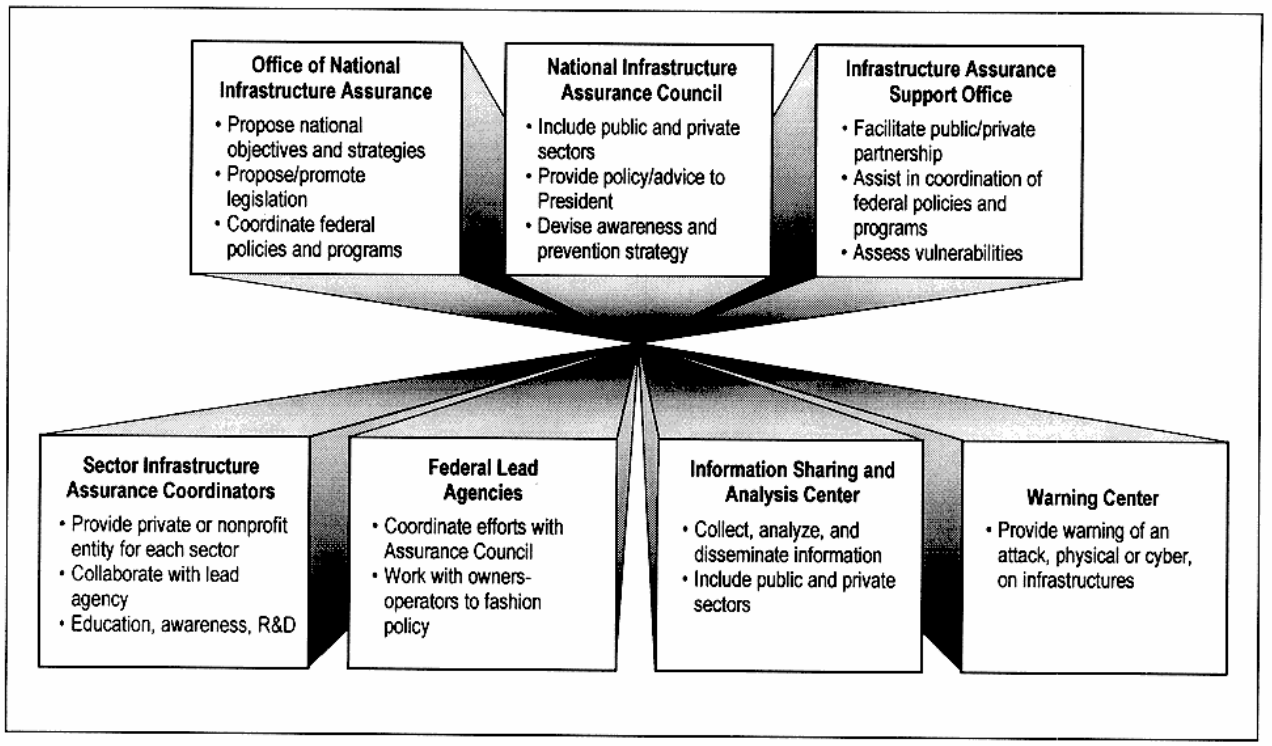

Figure 28

Proposed National Structure

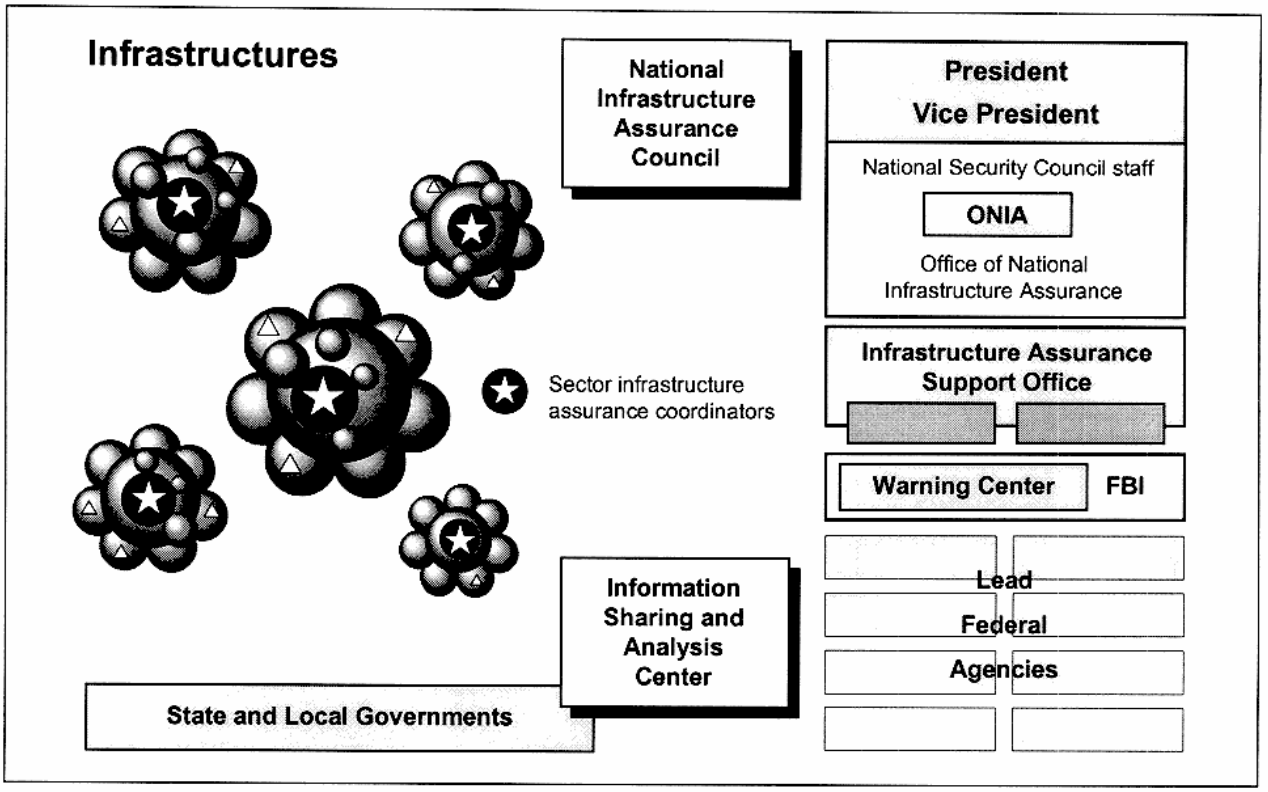

Figure 29

Infrastructure Assurance: Proposed

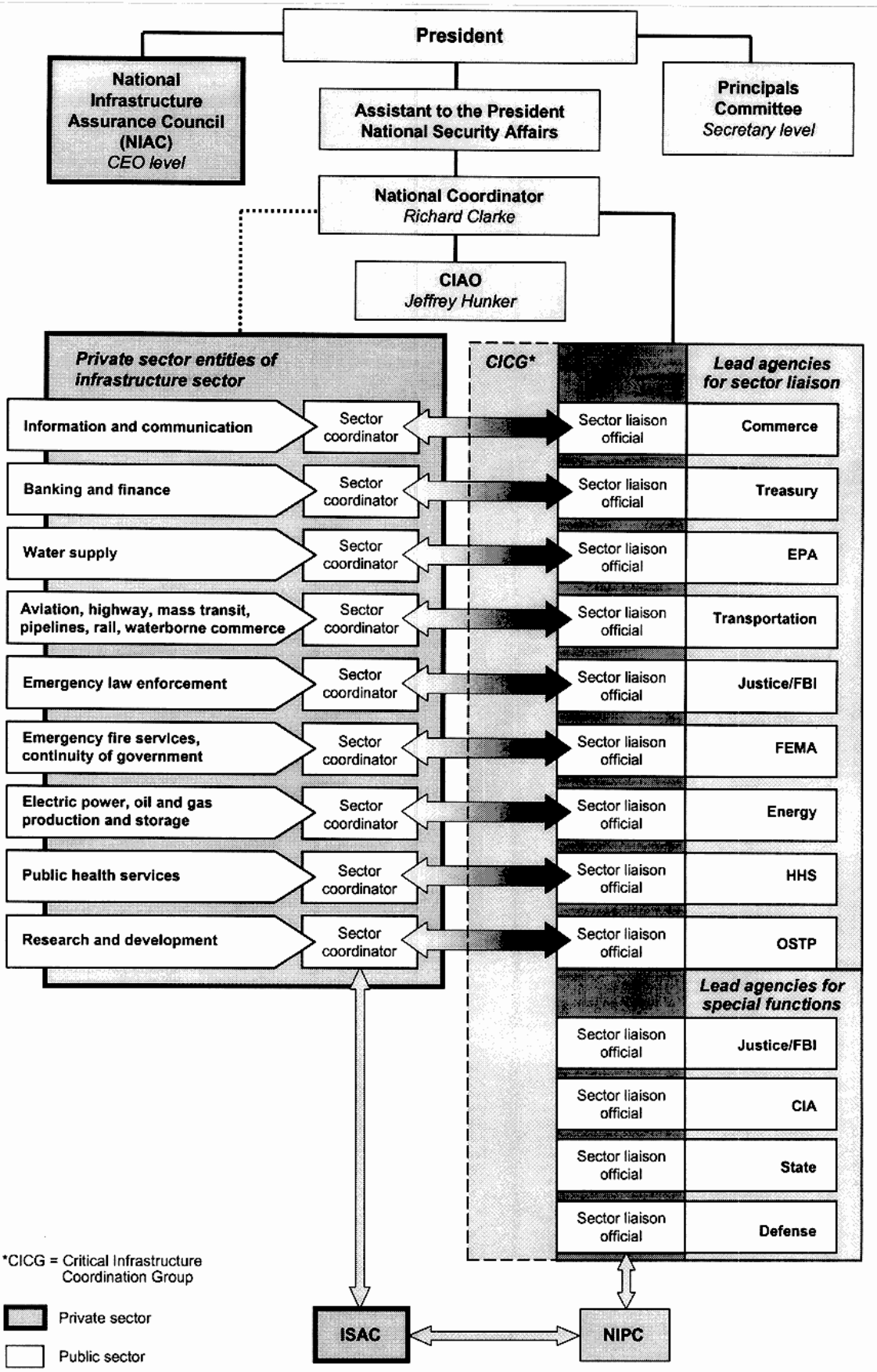

Figure 30
National Structure

we didn't envision that he'd carry all of the other responsibilities he has. He has the WMD (weapons of mass destruction) responsibility; he has the general terrorism responsibility; and now he has the cyber terrorism and infrastructure assurance responsibility. I think his position is unduly diluted. It was our view that the critical infrastructure focus should be a single responsibility. So, in that sense, I was somewhat disappointed. The supporting office, the Critical Infrastructure Assurance Office (CIAO) under Jeff Hunker, has been established. It has suffered from a lack of resources and personnel to do the kind of job that we envisioned. The lead agencies have been designated, but as far as I can tell little of their activity has made itself felt in the private sector.

In a nutshell, I've seen a lot of activity of the federal government trying to get its act together. Certainly that's important. The DOD is taking some very important and bold steps to secure its systems. Not all agencies have done as well. But I see little or no action in the private sector. There's been no action to establish the ISACs or the national council. We thought that with the establishment of the national council, the appointed CEOs would work with their peers to transmit the importance of this problem to the private sector and bring a national focus to it. That hasn't been done. Frankly, I've seen nothing from the bully pulpit to raise general public awareness of the problem.

So, that's a quick trip through it, to give you a feel of what we did and what we recommended (figure 31). I hope I haven't overkilled it.

Risk is shared among public and private interests.

Partnership is the foundation for infrastructure protection.

Figure 31
Conclusion

One of the things we recommended was that in the key critical infrastructure industries you use the equivalent of military two-man access control to the critical operating functions of the network, and that two people buy off on any changes. We recommended that the law be changed to provide that designated people in the critical infrastructures be subjected to background checks, and have what we in the military would consider to be security clearances. That was the way we intended to deal with the insider problem: that for certain key functions the CEO would use background checking and so on to better assure trustworthiness.

Oettinger: Let me raise what might be a counterargument to that and then see how you'd dispose of it. It goes back to the earlier point, which I agree with, about the difference between the private sector and the public. Some things you let go in the private sector because, what the hell, it's only money, and if you have to spend more money to guard against it than you would lose if it happened, you're likely to take a chance. I mention it in this connection because what you suggest raises costs implicitly or explicitly. If I do it country-wide it may not be a competitive factor within the United States, but I can see the private sector saying, "We're doing this unilaterally and therefore we will be at a disadvantage vis-à-vis the competitors from country X, Y, or Z." If it's done in X industry, which perhaps has some competitors in another industry, then they can say, "Well, they put us at a competitive disadvantage versus another industry or another company," and so on. Did that sort of argument get raised, and what was your counter to it?

Marsh: One of the first things you have to ask yourself as you enter that discussion is: What are you talking about in terms of cost for security? Are these substantial amounts? We tried to quantify that, and we're not talking about very large sums of capital investment. We're talking about the cost of good, solid firewalls. We're talking about the labor costs of good, talented system administrators. We're talking about rigorous enforcement of passwords, which is management

and involves no cost. We are talking about sensible use of encryption for critical functions. When we say critical functions, we saw some in the power industry actually moving to put SCADA (System Control and Data Acquisition) onto the Internet, all in an effort to save money. But they can't tolerate the denial of that control capability and yet the Internet is denied frequently. So now you could say, "Well, to put that on dedicated circuits is an additional cost of doing business." We don't view it that way. We think the Internet approach wasn't a sensible cost saving.

But the bottom line is that we're not talking about untoward investment costs to strengthen the security of our systems. Much of it is discipline. You know it well. Don't bring those disks from home and load them on your controlled network. No unauthorized access to the Internet in this organization where it isn't required, or use of sensitive information when the network is connected to the Internet, and so on. There are good solid security practices that don't cost a lot of money.

Student: How about extensive costs from lawsuits? The problem is being identified, and this possibility that they will also say "We can't do what we're supposed to do." Then it's not simply investing for protection. The great amount of money, I think, would be involved as a result of lawsuits. That is supposed to be increasing, and therefore the Congress is now talking about the notion of curbing the possibility of increasing lawsuits. The President threatened to veto it if the bill was presented.

Marsh: If I follow you correctly, you're talking about the Y2K insulation from lawsuits. Generally I think what you're saying is right. I believe that as the standards for system security are developed, either explicitly or implicitly, if people don't abide by those standards or don't maintain that standard of security, they're going to be liable to lawsuits. That's part of the awareness campaign. I think we must awaken the CEOs to the fact that they are going to be subject to lawsuits if they don't achieve an acceptable level of security of their systems.

Oettinger: I guess the thing that you can do would be to bring a good lawsuit. One of my good friends was the fellow who took what is now the LEXIS-NEXIS system out of the obscurity of being a toy of the Ohio Bar Association and into being a commercially viable database service. A *deus ex machina* that did him a great favor was someone who sued a lawyer for malpractice on the basis of failure to use LEXIS-NEXIS in doing a due diligence search of the database. The minute that thing hit the world, all the lawyers in the country felt compelled to get access to LEXIS-NEXIS to protect themselves. It required no legislation. It just required one lawsuit, and he laughed all the way to the bank. I'm puzzled why there has been no equivalent, because it wouldn't take major initiatives. It would just take somebody who said, "I've had a loss consequent on this."

Marsh: The CIAO is working with the big five audit firms today to try to make the security of their information systems a standard audit inquiry for all businesses. If they succeed in that, and if the auditors indicate that your practices are less than acceptable (incidentally, I've seen a draft of those standard practices from KPMG), that is, if you don't meet those standards, then you will be liable in the eyes of your shareholders for negligence. That's part of the awareness challenge. If we can get the auditors involved, and if we can get the insurance companies coupled into insuring against loss provided standards are met, I think we can improve the assurance of our systems.

One of the problems (we discussed it briefly at lunch) is that many of these systems are coming out of a regulated environment, and the regulated environment distorted the whole picture of liability. By that I mean that in the electric power industry, for example, the regulators set the rates. In the process of setting the rates and in return for minimizing those rates, it discouraged the industry from making investments. The result: if a bad storm's coming tomorrow, you know you'll probably lose power, and you'll lose your freezer full of food. That's on you. Maybe you have homeowner's insurance, but you can't go to the electric power guy. He'll tell

you it's an act of God: he can't help it that the power line came down. God did that.

That's all wrong. When you get to the unregulated environment, if he doesn't deliver power to you and you lose the food in your freezer, you have somebody to go after. That's why I say since many of these industries are coming out of the regulated environment, there is this distortion that exists where the forces of auditing, insurance, and liability don't play as in the true free market. But they will, and they're going to.

Oettinger: That's a very interesting point that had not occurred to me before. If I understand you correctly, you're saying that because these infrastructural organizations, by and large, were regulated, that as part of the trade-off in regulation they had immunities which ordinary businesses do not have: quasi-governmental immunity.

Marsh: Absolutely. You couldn't sue the power company ... or you could sue, obviously, but you'd lose.

Student: Before today we frequently came across this issue of cooperation or partnership between business and government. I'd be curious about your own practical experience. You said the commission was a very unusual entity when you created it. You brought in the up-and-coming people from the private sector. What was it like having those people working with people who have been members of the establishment and have different viewpoints? Did you come to a new understanding or were there difficulties every day?

Marsh: Let me tell you, it was wonderful bringing the private sector people in. They sure opened our eyes. It took a long time to turn a bunch of bureaucrats around. We were all bureaucrats, and had pretty set thinking. The early meetings were along the lines of: "Well, dammit, these systems have to be more secure, so lay it on them! Put a regulation out! Pass a law!" That's the first reaction of the bureaucrat: demand it and it will happen. It took the private sector to say, "Hey, you guys, you're talking about competitive businesses! People out there want to do right, and they will do right. They'll protect their resources, but if you know that their resources are in danger and they don't, then you have a responsibility to convey that in understandable terms." And on and on. I can't imagine what the results of our commission would have been had it not been for the private sector people. We wouldn't have hit this partnership thing, I swear.

Oettinger: You said "up-and-coming," and that sort of means "promotable." Let me put it this way. In the university business, one has a lot of interactions with the other parts of the private sector, the corporate world, and there are some real people in that. They're line managers, they run a business, and so on. Then there are vice presidents in charge of irrelevant academic meetings, and they are people to whom somebody says, "I don't really have time to deal with those guys; you go and spend time with them." I'm wondering which category you got. Were these "Washington representative" types, in charge of "keeping the Tsar far away from us," or were they real people?

Marsh: I know what you mean. To tell you the truth, we had both. We had two senior guys, one very recently retired from AT&T, and the other very recently retired from IBM. He had been their senior technologist. We had a young lady who was the deputy CIO (chief information officer) for PG&E, Pacific Gas and Electric, and really on the rise. She was very sharp. The guy from the Fed served at the VP level. So, it was a mixed bag, I guess. But they brought the views of the industry pretty doggone well.

Now, on the other hand, they got a view of national responsibility that I don't think they came in with. When they saw the scope of this and looked at it in a national security sense, they began to realize that the responsibility exists with the government to educate the CEOs. They acknowledged that the CEOs hadn't devoted the resources to this problem that it needed.

We talked to CIO after CIO who had gone to the CEO and the board trying to get resources and, consistently, wasn't able to make the case. That's the barrier to be broken. Somehow the federal government has to

carry the case to the CEOs by various mechanisms and help them understand that here's something they must face up to.

We said at lunch that our society, our nation, is just no good at solving crises before they happen. We address them well once we get in them, but we don't take steps to prevent them. That's the kind of problem you have here.

Oettinger: Of course, there may be a double whammy here, which goes beyond what you've just said. Let me try this out on you, because I have a good friend and former student, an alum of both the college and of the graduate school here from many years ago, who recently retired as the CIO of a major firm. One of the things he's been doing in the three or four months since he retired is he's writing a paper about the relationship between the CIO and the CEO. The problem that he raises is the whole matter of aligning the information technology capacity and outlook and strategy of the company with its business strategy. The theme is that this is broken and needs fixing, in that communication and common strategizing between the techies and the operators, to put it in military terms, is as bad in the private sector (from his point of view) as similar problems in other institutions. So, even if the CIO could be convinced to carry the message to the business side of the house, it might not be easy because it's one of a number of messages where the technical side and the day-to-day business side don't necessarily communicate. Is this guy a unique phenomenon?

Marsh: No. We heard similar stories from CIOs all over. They came to our many meetings, and they're just pleased as punch that somebody's carrying this cudgel and banner.

Oettinger: But they don't necessarily talk to the CEOs.

Marsh: That's right. They do not do so effectively.

Student: Let me point out one thing. I certainly see the gap between the industry people and the government side. But in DOD's annual report, which I read last month when it was released, I tried to look for any significant portion about the DOD's role in PCCIP or critical infrastructure protection, but all I could find were three paragraphs on critical infrastructure protection in chapter 7, which is about information superiority in space. The chapter itself doesn't even represent the basic question of the issue. How do you explain this apparent failure to address the issue in the DOD annual report, which is a very good means for educational outreach, on the one hand, while it is reported to Congress on the other?

Marsh: I haven't read that annual report. When I said that I think DOD is leading the pack (and it is) among all government agencies, I meant that DOD has had the wake-up call. They conducted the Eligible Receiver exercise; you've probably heard about it. It was a carefully planned inside penetration of their own systems to see what a team of just average ability could do. They did very serious theoretical harm to the DOD, and further, they kept the DOD in the dark. The DOD didn't know what was going on for two or three months of the four-month exercise. (This is unclassified and they've written it up.) They realized they didn't have the tools, they didn't have the information gathering system, and they didn't have the C^3 system to collect information and assess what was going on and then direct appropriate action.

That's really awakened the DOD. I know, for sure, they have a very aggressive program under way. Why they didn't give it more than three paragraphs I just don't know, but they're working at it very, very hard. I assume you heard about the DOD program from General Cunningham, Art Money's assistant.[3]

Oettinger: It also may be a report for one of the past years. It wouldn't necessarily have shown anything yet.

Student: My impression was simply that they were going to minimize that, hoping it would go away. On the other hand, the *New York Times* a week ago reported that the

[3] See General Cunningham's presentation in this volume.

number of people in the United States who were purchasing guns has increased 20 to 30 percent in the past few months. Apparently, they are buying guns to prepare for disturbances anticipated around the end of this year.

Marsh: I don't know about that.

Oettinger: The thing to do is not to go to high school on New Year's Day.

Speaking of the end of the year, there was a question earlier that hinted at the Y2K issue. Did your commission get involved in Y2K issues at all?

Marsh: We started down that road and then we decided there wasn't much of value that we could add to it, because it was fairly well understood. I think the Y2K problem is trivial as compared to this one. It's discrete. You know exactly what you're looking for. It's drudgery, but there's no technical challenge there.

We did say, though, with respect to Y2K, that we're opening up another avenue of vulnerability. That is, many companies who have up to this time protected their company jewels—that is, their proprietary software—very carefully, now are having to hurry and get anybody who can do some COBOL programming to fix things. Much of it's going offshore, and we think that can open up real problems. People can embed trapdoors and so on that can cause problems in the future. So we say, "For goodness sakes, try to assure that people who are going to fix your systems are trustworthy."

Oettinger: My concern is even before that. That's certainly a possibility, but the enormous growth in that market has attracted a lot of incompetent people as well. The sheer reopening of a lot of code is bound to increase the error rate.

Marsh: I must say that the bully pulpit's been used on the Y2K problem, and I don't think it needs it nearly as much as this larger problem does. I think the emphasis isn't in the right place. But, naturally, I would feel that way.

Student: In one of our readings it said that the United States was discussing the possibility of using a computer virus against the Iraqis. Do you recall that? I'm not asking whether there were certain questions about using the virus against the Serbs, but how well the Department of Defense controls the digital weaponry of the United States. For example, according to some rumors 20 years ago, one of the Soviet strategic bombers dropped a three-megaton bomb while flying over Soviet territory and nothing happened because it wasn't reported by the Minister of Defense. Now, let's say one of insiders in the Department of Defense releases a virus. Are there possibilities to control the spread of this virus? Can the Department of Defense introduce some antidotes or programs that would accompany this virus and stop the spread?

Marsh: I'm not an expert on viruses. But I do know that, at least to date, our virus protection, in every case, is against a defined virus. It's the undefined virus, tomorrow's virus, that we must devise methods to cope with, every time. To answer your question, just by the nature of viruses, I don't think DOD has good defenses against unknown viruses. For each one, you must encounter it, analyze it, and then devise and put out an effective counter. Maybe there is such a thing as a flexible antivirus capability that could cope with a great number of unknowns, but I haven't seen that.

Oettinger: In fact, the news from molecular biology is not encouraging on that score. My daughter is a professor of molecular biology whose specialty happens to be the generation of defenses against real-life viruses. The body is extremely efficient in countering strange new critters and building antibodies and so on, and that is controlled by a couple of genes that she and one of her colleagues discovered some years ago. But the bad news is that one of the reasons why colds last seven days is that it takes about that length of time not only for the body to figure out what's attacking it, but also to manufacture enough antibody to overcome the incoming virus.

Sometimes when you look for a biological model, adaptive models and so on give you at least something to aim for. Here, however, the news is that dealing with the unknown is not easy even after a gazillion years of evolution. So, it is possible that one might invent a smarter artifact, but neither nature nor nurture has figured that one out yet. It's a hard problem both in nature and in artifacts.

Marsh: A reason McAfee has been so successful is their network of informants around the world. They have a scheme whereby they get a new virus reported back to them, they go into panic mode for about 24 hours developing the counter to it, and then they get that out at the speed of light.[4] Reaction time is everything in that business. When I visited out there, I didn't hear any of the theoreticians talk about having a blanket antivirus capability.

Student: There's also a rumor in the industry that many of the people who design those viruses are on the payrolls of the antivirus companies.

Marsh: That's how they keep themselves in business (joke).

Oettinger: That's a reassuring thought.

Marsh: Entrepreneurialism at its best.

Oettinger: Put in a little pneumococcus and ...

Student: Is there any cooperation with the European agencies? I know that in Europe there is a lot of research going on in protection of information infrastructures under a different pretext, like fighting child pornography and stuff like that, but basically it's imposing controls.

Marsh: Gee, I'm glad you asked. I failed to mention that at all. One of the largest shortcomings of our effort was that we did not get into the international implications of this; we readily acknowledge that. This is not a national problem; it is an international problem. There are no such things as national infrastructures; they're international infrastructures, and so we must strike collaborative arrangements with all of our trading partners. That's a big step to be taken, and not much progress has been made. There are a few countries that are starting to get very interested in it. We reached out to a few of those—Canada, England, Germany, and Japan—but there's a long, long way to go.

Obviously, this is an area where we have to have international cooperation and cooperative agreements. The banking and finance world has been pretty good at this, because it's in their immediate business interest to have international arrangements on encryption, et cetera. I think the trade organizations are going to have to take the lead in this area. Much has to be done.

Oettinger: For those of you who are interested in pursuing that a little bit further, there's a book that I don't use in this course but that you might enjoy. It should shed some light on at least some of the mechanisms that the international financial community has used within the last decade, without changing national laws and so on, to come to a kind of harmonization in guarding against embezzlement and one thing or another. The author is Ethan Kapstein, and the book is called *Governing the Global Economy.*[5] It's a relatively sane, sensible, empirically based book. I don't know if you had the occasion to use Kapstein as a consultant for the commission.

Marsh: I don't think we did.

Oettinger: He's now at the University of Minnesota.

Marsh: There's a lady here at your school, Deborah Hurley, who was with the OECD (Organization for Economic Cooperation and Development) before she came here. Just as

[4] Network Associates/McAfee develops antivirus software, and also sponsors the Anti-Virus Emergency Research Team (AVERT).

[5] Ethan Kapstein, *Governing the Global Economy: International Finance and the State.* Cambridge, MA: Harvard University Press, 1994.

she was leaving the OECD, they were starting to address this topic. I don't know how much progress they've made.

Oettinger: Anybody who's in here could talk to Deborah Hurley, so that's a good point. She is here now.[6]

Student: We had another IOP (Institute of Politics) project among our students with her. They did their thesis for the FBI on, I think, commercial encryption. You might be interested in reading that thesis as well.

Marsh: I'm surprised nobody brought up encryption. We tried to duck that as best we could because we were caught between a very difficult series of administration positions. The way we came down, though, on this whole question of public key and who has access and who has ownership, et cetera, is that the government ought to lower the temperature of the debate. It should sponsor a large, privately developed public key encryption system that touches the public in a direct way, like Social Security. The government should turn it over to the private sector to develop a secure system and prove that the public can have confidence in it without the government having the exclusive control of the key, and that nobody's privacy is unduly impinged and so on. Some agencies of the government have suggested a number of pilot programs. We believe that the government ought to get behind one and get moving with it. It could, we think, do much to put this debate to rest.

Oettinger: Yes, that's a hard one.

Marsh: It's very hard.

Student: You had on the map the pipeline in Alaska (figure 3). Could you tell us more about what kind of infrastructure assurance methodology or policy you have toward pipelines?

Marsh: The controls are, as you know, very automated, and consequently they depend heavily on the SCADA systems that control the valving and so on. Frankly, they're not protected in any unusual way. We found them to be very vulnerable. We recommended steps, but the specific vulnerabilities and the specific steps to fix those are in the classified portion of the report.

They have other vulnerabilities, too. Some have important physical vulnerability problems that combined with cyber vulnerabilities make them exceptionally vulnerable. Much of their pumping hardware has little or no redundancy and consists of unique devices that have very long lead times for replacement.

Student: Since now most of Alaskan oil will be developed by a British company, it will be interesting to see how the U.S. government will cooperate with the multinational BP/AMOCO.

Marsh: And ARCO.

Student: Yes, I think that they bought ARCO as well.

Marsh: They're buying it, or at least they propose to.

Oettinger: There's a whole set of issues there in public/private sector collaboration that perhaps you can say a few words about. There's the question of who's the private sector, and does nationality matter, and does control matter? What is your thought or the commission's, personally or officially, or any response to that set of issues?

Marsh: We worried about it a lot. At the time we were in session, British Telecom proposed to buy MCI. We testified before whoever was hearing that case that should there be such a purchase, there ought to be in the purchase agreement provisions that they abide by specified security standards. We haven't specified any security standards to this point; they're yet to be developed. If they should include putting monitors on certain lines and so on, the foreign buyer ought to have to agree. If a foreign firm acquires a de-

[6] Deborah Hurley, director, Harvard Information Infrastructure Project, John F. Kennedy School of Government.

fense-oriented company, they have to agree to a special security arrangement such that they abide by U.S. laws and regulations regarding security. We felt the same should be included if a critical infrastructure were acquired. That's very easy to say and tougher than the devil to do. You're right, that's internationalization, and it's going to have to be addressed.

Oettinger: But it's another area where it seems to me that some competitive interests would be at odds with national security interests. I would imagine that a whole slew of American companies with an interest in doing business abroad would be against such regulations for setting the wrong example in terms of their negotiations with the Chinese government or whomever.

Marsh: But again, we're talking about our critical infrastructures, and we're saying that in case of the acquisition of them, or elements of them, we ought to assure their security.

Student: You emphasized the word "critical" several times. How can you say an infrastructure is really critical? I'm asking about your criteria for whether or not an object is critical.

Marsh: We operated on a pretty loose definition, which was that major damage or destruction of a major portion of that infrastructure would have a serious debilitating effect on the American economy or national security. It was up to us to refine that.

But it was generally defined for us. We were given the critical infrastructures. We were asked if we agreed with them or if we wanted others, and we generally agreed with the ones we were given. We think they are the fundamental underpinnings of our industrial society.

Student: Would it cost much money for the private sector to protect the infrastructure against certain digital attacks? Previous speakers have mentioned the threat of electromagnetic pulse (EMP). I do not know much about this phenomenon, but it seems that to install protection against these sophisticated things would cost a lot.

Marsh: It is a threat spectrum. I went over to the House and testified in front of one of the committees on science and technology. One of the congressmen was very hard over on high-altitude EMP and shouldn't we do something about that.

Well, it's unthinkable to protect against high-altitude EMP. The way we've protected against it in the past is that we've deterred it. I would put my resources into making sure that doesn't happen rather than assume that's it's going to happen and protect against it.

We looked at the lesser (less than nuclear) electromagnetic weapons as deeply as we could. I think we had all the available intelligence on that. I will say that such a weapon is still in the works, despite what you read. If it gets developed, it may be practical for some guy in a small truck to come around and zap out all of the Kennedy School's computers. Then we'll have to take steps either to deter it or, if you feel you can't effectively deter it, put in protective measures. Now you're talking screened rooms, I'd guess, and all that goes with that sort of thing.

As I said, we may get to a point some day when the federal government must do more in terms of incentivizing or giving investment breaks in one way or another. Today, we don't see that as a real threat.

Student: Are you saying that the United States is developing that kind of small truck, or that somebody else around the world is doing that and that the time will come when somebody can bring those mobile magnetic pulses somewhere near the Kennedy School?

Marsh: There are proposals, and you can read about them in the literature, to develop small electromagnetic generators, focus their energy by way of an antenna, and hide them in a small truck. We believe that's not yet achievable, in a practical sense. It's theoretically possible. We need to watch that development, and if they're successful, we'll have to work on how to counter them. The Russians advertise that they actually have a small explosive electromagnetic device. We do not believe they have a workable device.

Student: It seems that the national plan in some cases doesn't necessarily transfer to a

more local plan. In dealing with catastrophic terrorism, for example, there's always a local plan in place for local police, local fire, and the like, but in critical infrastructure protection, because of the interdependencies, it doesn't seem obvious that you would need a local plan. Fundamentally though, everything does happen at a grassroots level. So did you have the opportunity, or was there any point work in progress, to go to local communities and figure out their concerns on critical infrastructure protection and bring them into the process?

Marsh: The local communities are owners and operators of their own municipal power plants, for example. So we're back to information sharing. They want to be wired into the federal government's information flow. They want to know what threats they ought to protect against, what the best practices are, and what actions they should be taking. They feel isolated. They don't feel they're getting that kind of information today.

We proposed there be some local and state government officials on the national council that we recommended to facilitate information flow and address the concerns of the local communities and states. Because you're absolutely right: they're the first responders down there, and in many cases, they're the owners and operators. They own the emergency services in many cases, the 911 system.

Oettinger: Our local highway system is one of the infrastructures critical to our speaker's getting on an airplane this evening. If we're going to bear any reasonable responsibility for his making his plane, I think we need to bring this conversation to a close now, which I will do with this small token of our great appreciation.

Marsh: Thank you all very much. I enjoyed it.

INCSEMINAR1999

ISBN-1-879716-63-1