INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Cyber Threats: Developing a National Strategy for Defending Our Cyberspace
Mark C. Montgomery

Guest Presentations, Spring 2000
Charles E. Allen, Albert J. Edmonds, John J. Garstka, Timothy G. Hoechst, Hans Mark, Dale W. Meyerrose, Mark C. Montgomery, Scott A. Snook

July 2001

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 1-879716-74-7 **I-01-1**

July 2001

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Anonymous Startup
AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz•Allen & Hamilton, Inc.
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
Critical Path
CyraCom International
DACOM (Korea)
ETRI (Korea)
Fujitsu Research Institute (Japan)
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
High Acre Systems, Inc.
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
NMC/Northwestern University
PDS Consulting
PetaData Holdings, Inc.
Research Institute of Telecommunications and Economics (Japan)
Samara Associates
Sonexis
Strategy Assistance Services
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Upoc
Verizon

Cyber Threats:
Developing a National Strategy for Defending Our Cyberspace

Mark C. Montgomery

April 13, 2000

Commander Mark Montgomery is director for transnational threats at the National Security Council, where he serves in the office of the national coordinator for security, infrastructure protection, and counterterrorism. He helps to coordinate national security policy in the areas of information warfare, counterterrorism, and information security training. He is also a surface warfare officer in the U.S. Navy. From 1988 to 1998 he served in a number of shipboard assignments, including as a division officer on the USS Bainbridge, *operations officer on the* USS Leftwich, *as reactor electrical assistant on the* USS Theodore Roosevelt, *and most recently as executive officer on the* USS Elliot. *A resident of Sunapee, New Hampshire, Commander Montgomery was graduated from the University of Pennsylvania, receiving B.A. and M.A. degrees in history and political science, and was commissioned in the U. S. Navy through the Naval Reserve Officer Training Corps program. He subsequently attended Oxford University, where he earned a master's degree in modern history. He has also completed the naval nuclear propulsion program.*

Oettinger: There's a change in our program today. Our speaker is not John Tritak, who has been preempted by the White House. He called yesterday and said he could not make it. That's the bad news. The good news is that Commander Mark Montgomery will give the briefing. For those of you who were not at the lunch, here is Commander Montgomery's biography. Now let me just turn it over to Mark. We're delighted to have you here.

Montgomery: I plan to talk about what we're doing in the White House and in the executive branch of the government in developing a national strategy for defending cyberspace. I would propose about a 20- or 25-minute briefing, then questions for an hour. It might go a little bit longer if you have a lot of questions. If I say something that you find completely unsatisfactory, please just raise your hand, and I will stop and try to explain it while I'm still on that train of thought.

One thing that I think is fair to say at the outset is that at the National Security Council [NSC] we're learning that computer security and critical infrastructure protection are national security problems that cannot be handled by law enforcement or the Department of Defense [DOD] alone (**Figure 1**). This makes them practically unique. There is only one other issue like this where the FBI, or the Department of Justice, or the State Department, or the DOD just can't handle an issue or a threat on its own: the issue of weapons of mass destruction [WMD] preparedness, or how we protect our homeland against chemical and biological weapons. They

Figure 1

both really are issues where we need a new national security template for protecting ourselves against an emerging threat.

WMD preparedness and cyber security also share the theme of being ambiguous or asymmetric attacks. This is to say that when you have a cyber attack or a chemical or biological attack, you may not know it's an attack for the first few days. Computer networks and systems fail every day. The government estimates that the failure rate is well under 1 percent: 0.1 or 0.2 percent of its computer networks suffer outages every day. The system goes down, and the system administrator has to reboot it. Why did it happen? Sometimes it's gremlins, mostly it's systems being improperly aligned or having software loaded on them where it doesn't belong. Sometimes it happens for no apparent reason.

About two or three times in the last year, when there was heightened readiness for other reasons, the DOD informed the NSC of major computer networks or systems in the intelligence community having shut down. In each case they called back about three or four hours later and said, "What happened was that we loaded some software, or an inexperienced technician did something, and that's why the system went down." The source of a computer network failure can be really ambiguous.

The other characteristic that WMD preparedness and cyber security share is the likelihood of nonstate targets. The idea is that if you were going to carry out a cyber attack against the United States, you wouldn't say, "You know what? I'm going to take out the computer networks on the *USS Eisenhower* in port in Norfolk." It's very difficult to do: the ship is actually at least mildly isolated, in cyber terms, from the government, and it's self sustaining. It's got its own electrical power plant and communications and can go out to sea. Adversaries would be more effective if they attacked a region's electrical power grid or the telecommunications system. They could also attack our 911 system or the electrical power that supports it. There are insurance adjusters who can tell you how many more people would die in an hour than would die otherwise because of the lack of rapid or efficient response by the police or emergency services if you took down New York City's 911 system.

Critical infrastructures are nonstate targets. The government doesn't own the electrical power grid. It doesn't own the telecommunications systems. Some of these systems we don't even regulate much anymore. So many of these infrastructure systems—the electrical power grid, telecommunications, oil and natural gas, and emergency services—are not only not operated by the government, but also are not aggressively regulated. Transactions over the Internet are not regulated, and they're not taxed either. In some instances private sector computer networks are not really even understood very well by the government because of their complexity, size, and uniqueness.

The potential for domestic targets is particularly challenging for the government. Our military has worked hard since 1820 to extend the initial contact point with the United States away from our borders, but the cyber threat is really pulling it right back into our homeland. It's true of WMD as well, but with WMD you still have to physically deliver a weapon or its components to the United States, which is more difficult than delivering a cyber weapon. To deliver a computer virus to the United States, you just have to put it in play on the Internet, and it will get here on its own even if you didn't direct it, or you started it in Europe. The Chernobyl/HIV virus last year did eventually get here, but not to the extent it hit Northeast Asia. So there is a threat to the domestic United States. (That's the Chernobyl/HIV virus on the computer; I don't want you to confuse it with a chemical or biological threat.)

What kinds of cyber threats does the federal government look at? I have listed several of them here [Fig. 1]. First are hackers and computer criminals, because they really are the most prolific threat we face today. I know you constantly hear the White House putting the cyber threat in the national security perspective, but the reality is that 90+ percent of the known and developing threats and attacks happening day to day are criminal in origin. They are not foreign government information warfare programs or terrorist information warfare threats. They are people stealing money or stealing proprietary data. That shouldn't surprise you, because you can make a living stealing money or stealing proprietary data out of computer networks.

Computer criminals are undergoing a version of Moore's Law. Do you all know Moore's Law? It has to do with how fast computer networks replicate and improve, and it predicts that the size of the Internet will double every eighteen months.[1] Unfortunately, computer crime is frequently not reported to the government. Computer crime, as reported in private polls and analyses of the industry, doubles every twelve months. That is to say, a private polling company looked at 50 computer companies in 1998 and found that about $75 million in computer crime occurred in those firms. In 1999, the same 50 companies suffered nearly $150 million worth of criminal damage. I say "damage" because the loss of proprietary data is damage in the sense that it means lost revenue in the future when another company is using your formula or your plans.

---

[1]According to the ZDNet Webopedia, "Moore's Law is the observation made in 1965 by Gordon Moore, co-founder of Intel, that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the foreseeable future. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every eighteen months, and this is the current definition of Moore's Law, which Moore himself has blessed. Most experts, including Moore himself, expect Moore's Law to hold for at least another two decades." URL: http://www.zdwebopedia.com/Microprocessors/Moores_Law.html (Accessed on Feb. 25, 2001.)

I previously predicted that this rise in computer crime would level out last year. We saw that it had doubled over three years, and I thought that it couldn't double again in 1999, but I was wrong—it did. I have no reason to believe now that it won't double again in the year 2000.

The amount of crime being reported to law enforcement is also doubling, but it's still only 10 or 20 percent of the actual computer crime that occurs. Many companies don't report cyber crime to law enforcement. They do report it to their insurance companies, but the insurance companies also don't share that information with the government, for the same reason that the companies don't: it creates unwanted publicity

Student: Presumably, it will continue to go up until the cost of the crime equals the cost of the enforcement. Have you done any modeling to look at what that point will be?

Montgomery: Yes, that's interesting. The reason it is not being reported is that these are very competitive times. For instance (this is fictional), the credit card companies are afraid that if Citigroup says, "We've had 50,000 credit card numbers stolen and $27 million run up against them," even though they guarantee everybody that they would make restitution for those losses, the next time you get a credit card you're going to go to Bank America. So it's not a perfect physical security model like the one you described. I do accept your general tenet, that if we can give them computer security cheaply, they will accept it. That's for companies that have a long-term infrastructure involvement, which includes Citigroup or Visa or American Express.

Let me give you another example: eBay, E*TRADE, and the vast majority of other e-commerce sites are built on the concept of no infrastructure. That is to say, the reason that Amazon can sell you a book at $17.30 instead of $18.50 like Borders is that they don't pay for a big retail store. They don't pay for a guard to stand outside the store, and they don't pay for the alarms that go off when you steal a book.

Oettinger: I had a story yesterday with direct involvement, and it involves you, too. We have a researcher from Australia who has published a book, and the question was how to make it available. We said to her, "Gee, it would be nice if maybe you could market it through Amazon.com so we don't have to store it here." She said, "Oh, we're way ahead of you. We are distributing it through Amazon.com, but Amazon.com won't distribute it out of Australia unless there is a local distributor." We asked, "Who is the local distributor?" She said, "I am." I asked, "So where is your stuff?" She said, "Down in my office."

Student: It's "just-in-time inventory." You don't pull things in until you're selling them out.

Oettinger: Either way, I end up paying for the storage of her stock, whether it's sold by Amazon.com or directly. They're smart as hell.

Student: You push inventory back to the manufacturer.

Montgomery: The impact for us is that when we go to these companies and say, "Hey, you need computer security" (and we did; we went to all of them last year), they think, "Security equals infrastructure, and infrastructure equals overhead and overhead equals failed business." Amazon still isn't turning a profit on books. If we tell them to increase their computer network infrastructure significantly, they think it's actually going to put them further away from making a profit on books, so they're not as accepting of the idea of putting extensive computer security on there until they experience a significant disruption of services.

Let's fast-forward to February of this year. Three or four companies had a significant disruption of computer services. When they did, these companies—eBay and a few others—came running to the government and asked, "What are you going to do about it? How are you going to protect my security? Why didn't I get a warning?" The reality was that we did warn people about someone distributing denial-of-service tools in December 1999. This attack eventually happened in February 2000, and most of these companies did not demonstrate too much institutional memory for security issues. They didn't accept the warning that gave them 45 days' heads-up to protect themselves against distributed denial-of-service attacks. They did nothing. It's amazing that they weren't taken down more seriously. I'll talk a little bit more about that issue later.

Student: Why does increased security mean more infrastructure?

Montgomery: There's more overhead cost to the business. It means procuring firewalls and intrusion detection monitors, and having system administrators to make sure the firewall software is being updated. They actually don't buy a person for that. Mostly, they have to buy a service that constantly evaluates their firewall and intrusion monitors and makes sure they have the latest upgrades.

Student: It doesn't necessarily mean changing their distribution system?

Montgomery: It will slow it down slightly. My personal belief is that almost no enterprisewide security system slows you down so much that it's not worthwhile. When I say "slows you down," it slows you down milliseconds per transaction. Admittedly, that adds up over a day when you're Amazon and you have millions of transactions, but I don't think it's a significant impact. Another reason is the up-front cost of buying the firewall, the intrusion detection systems, and the software. Many companies would much rather that we just told them there wasn't a problem, and that we assured the American people they could continue investing in them, or purchasing their products, and using their credit cards to do it.

This is not an issue many entrepreneurs thought about three or four years ago when they were starting up. When you have only $1 million to start out, you don't want to spend $150,000 against criminals and hackers you are not sure even exist.

Hackers are another form of criminal activity. Can they do damage? Yes. There was a case about two and a half years ago when a teenage hacker broke into a public telecommunications switch and turned it off. That switch controlled the voice communications for a regional airport's air traffic control system. Luckily, those air traffic controllers had actually planned for and thought about this sort of occurrence, not in terms of a hacker but in terms of a lightning strike taking out the telecommunications system. They had personally owned cellular phones, and they would call an airline's base, the airline would call up to their pilots, and the controllers could talk to the pilots and perform air traffic control. That is not the normal Federal Aviation Administration [FAA] way of controlling aircraft! Imagine if it were Logan or LaGuardia or National Airport in Washington, D.C. You'd have significant safety issues. Clearly, hackers can create damage.

The DOD has had its share of hacking incidents as well. "Solar Sunrise" was a comprehensive downloading and reconnaissance (by a hacker) of our military logistics systems in February 1998. This happened to coincide with one of our frequent buildups for a potential confrontation with Saddam Hussein. The cyber intrusions were coming in from an overseas ISP

[Internet service provider), and there was significant concern of an imminent cyber attack. It was actually two kids in San Francisco and one teenager in Israel, basically doing a check of what U.S. troops and equipment were moving to the Gulf. They were just checking out of their own personal curiosity, not because they were part of Saddam Hussein's intelligence apparatus. But we were unable to stop it from happening, and for quite a while we were unable even to determine where it was coming from. Most military agencies that were being exploited didn't detect what was happening at all. That's a significant issue for us.

Virus propagators also benefit from Moore's Law. Last year, viruses were estimated to have caused $12 billion in damage worldwide. The year before it was between $4 billion and $6 billion, although these numbers are hard to determine. I will predict that the damage from this malicious activity will not continue to double, and I'll tell you why. There's better distribution of antivirus software going on. Just basic antivirus software will help a lot. I saw yesterday that the Chinese government actually approved or validated a major U.S. antivirus product as a tool for virus management for companies inside the People's Republic. Still, the estimated $12 billion is a lot of damage. It has a significant economic impact.

The next types of cyber threats are foreign government programs. There are two basic types of foreign information warfare programs. One is more or less espionage based, where they're using cyber techniques as a new espionage tool to garner military intelligence or economic information on a country. The other is that some countries look at cyber warfare as maybe a way to conduct warfare against the United States or other countries that have developed computer system-driven infrastructures. The National Security Agency [NSA] made a widely publicized comment that there are 100+ countries developing information warfare capabilities. I think that number includes a lot of countries only on the basis of the estimation that they use computer systems to enhance their military or intelligence capabilities. In other words, they cast a very wide net when they say 100+ countries.

The final threat is from terrorist organizations, but we actually haven't seen a lot of terrorist information warfare and I can't explain why. I would certainly argue that cyber attacks would clearly be a great tool for terrorists. Just as chemical and biological weapons would create massive dislocation and loss of faith in government, cyber warfare could do the same thing. However, other experts argue that terrorist groups are looking for a more explicit target than cyber attacks can provide. They want to be able to say, "We did this." Taking down a 911 system, so that maybe three people die in a car accident because they aren't treated rapidly (that's a secondary effect of taking down a 911 system) may not give the terrorists the kind of publicity or the effect they wanted out of it. In any case, we haven't seen much use of information warfare by terrorists.

Student: Are you including under "terrorist information warfare" the capability for the terrorists or organizations to put their propaganda on the Web?

Montgomery: That's interesting. Yes, we have observed numerous terrorist organizations using Web sites to do recruiting or spread propaganda throughout their localities and in Europe. Interestingly, at least to us, there is one terrorist or former terrorist group right now, Aum Shinri Kyo (the ones who conducted a Sarin gas attack in the Tokyo subway), that went into the computer software business. I guess they got out of the agricultural products business with some help from the government. They're getting a pretty good market niche in Japan, and the reason is

their cheap labor: when you employ cult members you tend to get cheap labor. I think there's some level of embarrassment in Japan. It's been revealed that Aum Shinri Kyo sold some software products to government law enforcement and national security agencies. Having said that, if you check the software out and you feel it has no trap doors in it, I think that's definitely "buyer beware." That's an interesting problem for Japan.

After addressing all those potential cyber threats, let me pull back and say that the biggest problem for the United States, from the viewpoint of both national security and cyber crime, is still the insider. The reality is that 60 to 65 percent of computer crime is conducted with the assistance of an insider. That's a heavy percentage. It makes sense. If you want to get inside somebody's system, the best way to do it is to ask somebody to give you his or her password or let you know the dial-up number and modem port to gain access to the system. It takes a lot of the challenge out of hacking. Plus, once you get in, sometimes you need help moving between systems, because a lot of people are denied levels of access within the company, so you may need help from an insider to get around the network after you have hacked your way in.

Oettinger: I must underscore the importance of this point, because there's such a fascination with technology that this notion that the people are still the most important source of both strength and vulnerability often gets lost. If you look at the cryptography literature you get the sense that it's strictly a technology game. Historically—and this goes back as far in history as cryptography does—systems rarely get broken by technical prowess. They get broken by somebody being stupid. This was true in World War II. Some operational goof leads to the breaking of a code, and so, almost wherever you look, most of the failures have a lot more to do with people than with some kind of technology.

Montgomery: I can't complain. Enigma and Purple were broken in part due to the physical theft of systems that allowed people the cryptological access. In fact, I could go on and say that in computer network espionage, our biggest concern is that you can flip an insider who can get you access. When you think about physical espionage, let's say that I break into your office, whether you're a company or a government, and I steal everything in your safe. I just obtained a fixed amount of material: maybe it's fifteen documents; maybe it's thirty documents. You may or may not know that. If I photographed it, you may not even know I have it, but that's all I have. I don't have any special ability to get back into your safe. I've got to break into the building a second time to get into your safe again.

Now, let's say I break into your software system, your SIPRNet [Secret Internet Protocol Router Network], your classified secret system, or your company's proprietary research and development system. I'll steal everything that's there, plus I'll leave a trap door so I can get back in a new way. Even if you figure out I got in and you block that original way, I've left a back door to return in a new way. Computer network espionage really offers the opportunity for highly successful, repetitive espionage, basically until you replace the whole software system, if I can put in enough back doors and trap doors.

The insider threat remains a problem for us. If you think about who the people are who have done the most damage to U.S. national security in the last twenty-five years, they weren't foreign national spies. They were insiders like Aldrich Ames and Warrant Officer Walker who were flipped, and career civil servants, military officers, or people with twenty-five years of TOP

SECRET/SCI clearance who were compromised and then gave up information. Insiders are really our worst problem.

Student: I'm about to write up the Japanese case you mentioned, on the Aum Shinri Kyo cult. The group actually did not contract directly with the defense agency or some Japanese government agency. They basically were subcontractors, and the major contractor was a company like NEC or something. Is it possible to screen that kind of small subcontractor to a major company?

Montgomery: You highlight a difficult problem. We faced the same thing during Y2K [the preparations for the Year 2000 conversion]. Every worker who did Y2K remediation on the classified systems of the intelligence community and DOD had a TOP SECRET/SCI clearance. We tend to have enough money to take care of our SECRET systems and our TOP SECRET systems, and even if we don't we end up putting the money into them. That was certainly not the case with unclassified government systems and private sector systems, but think what would happen if we lost control of our unclassified systems or if our companies' databases were compromised! We're back to the issue of how much you are going to invest in security. It's very expensive to do personnel clearances on all the workers who touch your software. In the United States—and I'm sure this is true overseas as well—the government doesn't own the code writers. The code writers are all subcontracted civilians. We even do that on classified systems now, but at least we check to see that they have the appropriate clearance.

I recall there was a recent case involving the FAA's Y2K upgrade. Part of their Y2K remediation was done by thirty-two foreign nationals on H-1B visas. That didn't meet the normal security requirements. Although we have never classified the FAA software, it's important safety software. This failure to control subcontractors is prevalent in the unclassified systems of government and the private sector.

It's very challenging for a company to insist on a clearance, even beyond the legal aspects. In the United States, at least, you have a constitutional problem. You can't just slap a polygraph machine on every person who works for your company or does subcontracted work for your company. You will pay a heck of a lot for subcontracts if you start saying, "I want to polygraph all your people to make sure they're not putting in malicious software."

Actually, something I'll talk about later on is developing tools that search for malicious code that someone might have installed. Those tools are not as close as we would have hoped. They're not a year or eighteen months away; it will be several years before you can use those tools. Back to your point—you are correct that subcontractor work is the most difficult to monitor, and we have the same problem in the United States that the Japanese government faces.

Just a final thought on cyber threats: individuals can create enormous damage. The guy who created the Melissa virus did $80 million in damage.

Student: What was the Melissa virus?

Montgomery: The Melissa virus hit about nine months ago. It was started by a guy named David L. Smith. He was somewhat sloppy, and law enforcement was able to trace one of his virus propagations to his own computer so the FBI actually found him fairly rapidly. They found him in about a week, which is pretty good for the FBI. The vast majority of these take six months.

Student: Do computer systems have a way of signaling the users if the security of that computer has been breached, similar to a pilot knowing he's being locked on and therefore that he is about to be fired upon by the enemy?

Montgomery: It depends on the quality of the software you have installed. The vast majority of computer systems with current enterprisewide security management systems (if they even have one running) can be tricked into not sending the alert and then having the footprints erased so that no one knew you were in there. There are ways to break in. You can enter as the system administrator, which would not send an alert. It would say, "Ah, it's my maintenance man here to help me." When you get in that way, you can carry out whatever nefarious activities you want.

Student: Isn't this what you were talking about when you mentioned the insider? For the non-U.S. government employee, if you're working on a government contract, there are legal issues involved requiring security and background checks.

Montgomery: That's what I said. But for private sector companies you have more difficulty polygraphing randomly without a cause—without evidence that justifies a polygraph.

Student: Just getting a full background check is difficult.

Montgomery: Yes, except that there are ways. In other words, when you're hiring your walk-in physical security, you can insist that they not have any felons in their group. There are some things you can do. But you are right. You are limited there. Really, the solution is what I mentioned earlier, which is developing software that will detect malicious code.

Student: You have the right not to hire people because they belong to a terrorist group.

Montgomery: That's correct. Acknowledged terrorists actually are one group to whom I think we can deny federal employment. You certainly can't do it on the basis of what nationality or ethnic group they belong to. I'm glad we don't.

This material on cyber security is a bit repetitive (**Figure 2**), but just to bring that together, there wasn't a big vote or a referendum where we decided, "Okay, we're going to entrust national security, economic stability, this great growth, to Sun Microsystems and Microsoft." But that's effectively what happened as a result of the information technology [IT] revolution. Cisco has 80+ percent of the router market. Microsoft has between 75 and 95 percent of the operating system market, depending on how you calculate it. Believe me, in the military I worked with Tomahawk missiles on an operating system that you could essentially obtain off the shelf from a private sector company. The operating system code had been tailored, but it was basically private sector, commercial off the shelf. There are lots of military examples of dual-use technologies like that. We are rapidly becoming dependent on them.

As a nation we have benefited fantastically from the IT revolution. Seven percent of our economy—the IT investment of our economy—has provided 30 percent of the growth over the last decade. That's the same part of the economy that we depend on for running our infrastructures and protecting our national security. So, we've benefited from it, but it's created a risk.

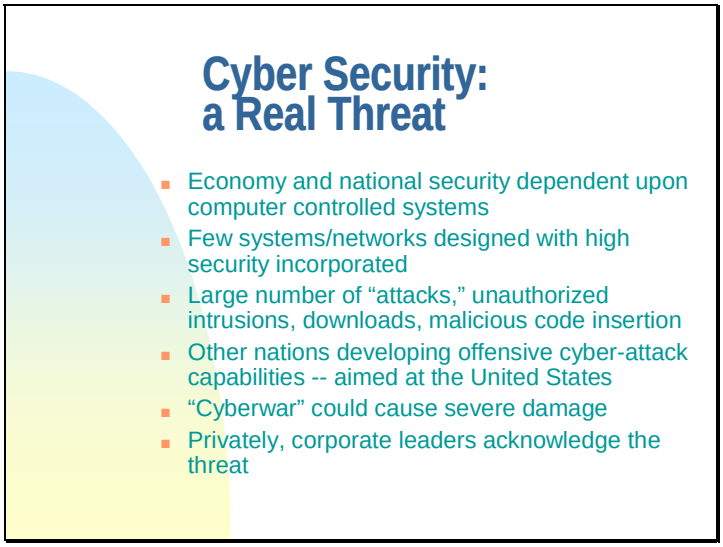

Figure 2

The reason it has created this risk is that few of these computer systems or networks were designed with security in mind. The Internet was designed by ARPA,[2] and the way they had security in mind was that there were only ten people on it. The terminals were given to trusted agents, people we trusted. (The irony now is that those same agents, usually university nets, are frequently the worst security violators among U.S. ISPs.) We didn't build ARPAnet with much additional security, and we rapidly went from ten or twenty ARPA terminals to 150 million computer systems in the United States (and the number changes every couple of days), so obviously it's a little late now to say, "You, know, we need to install security from the ground up." That's not going to happen, so what we're doing is putting a cheesecloth of security over it.

We hope that as we develop the next-generation Internet, we are going to put security in from the ground up. But sometimes when we go to those next-generation Internet meetings and start to say, "Hey, we really need security here," we can see people going, "*Ugggh*. That's going to cost. That's going to be a problem. That's going to slow this system down." You've already seen push-backs against security, even though they know the threat, and these are smart people. They have trouble saying, "Yes, we need to put security in from the ground up."

Oettinger: This is one of those places where the military sense of national security and the economic issues really overlap. If you're going to pay for security in some nontax way, then it is a lot easier to do that with a monopoly structure. In the good old days of telecommunications this was a nonproblem. Any time the U.S. Defense Department needed some security added, somebody picked up the phone and talked to one guy at AT&T, and he said, "I'll take care of it."

How did the bill get paid? It got spread across the rate base. It made a hardly perceptible difference on anybody's phone bill. It never required a congressional appropriation. Now, a Microsoft grew up out of a different tradition but could do it if it remains, as alleged, a monopoly. If you break up Microsoft you then have to start paying for security, and you have heard how

[2]The Internet is an outgrowth of the ARPAnet, developed in 1968 by what was then the Advanced Research Projects Agency [ARPA], now the Defense Advanced Research Projects Agency [DARPA].

refractory industry is about that. So it's a place where there is a strong linkage between industrial policy and national policy.

Montgomery: Actually, at the National Security Council [NSC] we're pretty decent friends with Mr. Gates. We visit him and talk with his security people a lot. We need them. A lot of our military systems and most of our private sector systems are driven by his software. He certainly doesn't do our bidding, though. On the humorous side, I've seen some recent open source information from the People's Republic of China saying there's a lot of concern over the use of Microsoft products, because the Chinese believe Microsoft may be working for the U.S. government. I couldn't think of anything less likely than Microsoft conducting espionage for us. Right now it's estimated that the federal government purchases less than 2 percent of software systems nationwide. We are no longer a market mover in software. The government saying "We need this" does not matter.

That is not the way we're used to having infrastructures move in the United States. When we thought in the 1980s we needed to have point-to-point encryption in telecommunications, AT&T created the infrastructure and started it nationally. They just did it. You're right, they spread the cost over everybody and you really didn't see it. I guess if there is enough defraying of costs over everybody you start to see it, but it didn't come in. Now, AT&T doesn't hold the national government contract for the Federal Telecommunications System. MCI and Sprint won it in the most recent bidding.

Student: Where is the threshold established when the cost of an action versus security is at equilibrium, so it doesn't matter at that point?

Montgomery: I guess you have to believe in the cyber threat. You have to believe that it will do real damage to your company. I'm going to talk in a few minutes about reconstitution, so let me address that there. That's why I was holding off in answering, because it will come up again and again: at what point do we strike a balance where people say, "Damn it, I'm going to invest in this!"?

Student: Not only that, there's a model there. That is, we've been down this road before, in the 1970s, when credit cards basically took over how we pay for goods and stuff. It's astonishing how easy credit card fraud is. There are some very easy things they could do to prevent it, but it turned out that the cost of preventing credit card fraud exceeded the cost of the fraud itself. So we have a model there for how this works, and basically what happens is that until they equal each other, once the cost of the fraud equals the cost of the prevention, that's where you start working on prevention.

Montgomery: Another aspect of this is that credit card fraud is a specific economic issue, but I could not make a national security argument for credit card fraud. I can make a national security argument that the same tool that would allow me to break into Citigroup and steal a credit card number would enable me to damage national security.

Oettinger: I have a problem with the way you phrase the question. It's precisely what Mark has put his finger on: it's not just a dollars and cents thing, and the perceptions are slow to change. During the Ford administration, when Nelson Rockefeller was vice president, he made it a personal crusade to alert the United States to the fact that the Soviets were listening in on U.S.

phone conversations, both military and commercial.[3] You can find a report of his out in the public domain, and he wrote an impassioned introduction. No one paid any attention to it. This was not on anybody's burner. Now you hear a guy from the White House giving you the sense that, "Boy, at least for a whole piece of the U.S. government, with a national commission, et cetera, it's a big deal. It's a front-burner thing," but the general reaction is still "ho-hum." You're dealing with something where perceptions aren't even yet of dollars and cents. This is thirty years after the first trumpet call, if you will. So there is a perception issue that is not present in the credit card case. I don't know if Mark will have any thoughts about how to get us off that in less than another thirty years. There's a different problem, which I don't claim to understand. I continue to be surprised about how "ho-hum" this set of issues is.

Montgomery: I'll talk about that a little bit. I hope things are changing. We will see.

There are a large number of "attacks," and I say that in quotes because a lot of these attacks are just probes. DOD articulates things in a very threat-driven way, so they call them attacks. Just to give you an idea, DOD had about 22,000 probes or penetrations or removals of information in 1999.

Student: Basically 22,000 unauthorized accesses?

Montgomery: Exactly, and those are the ones that they know of. I am sure there's a significant number of additional intrusions that they didn't know occurred. There are tricks of the hacking trade that the DOD doesn't know about yet. There are tricks of the trade that they do know about, but they haven't installed the latest software on their intrusion detection systems so 22,000 is the low end. I can't even tell you how many intrusions the rest of the federal government had, because we don't all have intrusion detection systems running.

I will tell you a good story. We went to the General Services Administration and said, "Listen, we want to procure some intrusion detection systems that cost about $60,000. We just want to buy two systems, and then have a contractor monitor them for a couple of months and see what happens. Tell us a couple of agencies." So we went to the CIO [chief information officer] of a federal agency, and he said, "Sure, we'll do it." We went to their leadership and said, "We're going to install this system," because we had to get their permission to look at the data. They said essentially, "No one's going to look at this stuff. No one cares about these federal agency Web sites. Everything we have is just as available on the Web. It's right there. You can look at everything."

The agency installed these intrusion detection systems and monitored them. The agency started to get all kinds of hits on them, and they occurred at the end of the month—most frequently at the end of the quarter. When I went back and asked the CIO, he said, "This is exactly what I expected. It's because I publish business indicators at the end of the month. People want to go in and access them and make financial decisions before the data are publicly revealed."

So, there it is. This federal agency does not provide national security information, but it has really important information and people want to access it illegally and obtain that information.

---

[3] *Report to the President on CIA Activities Within the United States* (Washington, D.C.: U.S. Govt. Printing Office, 1975). Also known as the Rockefeller Report.

There is a great deal of really important information on unclassified government systems. Think about the National Airspace System for the safety of flight and control of aircraft, and the National Weather System, which contributes to the National Airspace System and lots of other safety systems. The Food and Drug Administration has drug reviews going on. The National Institutes of Health have a lot of research and development databases where many people are contributing to group work at the same time. The Department of Labor, the Department of the Treasury, and the Securities and Exchange Commission all have economic indicators and information. The FBI has your fingerprints. The DOD, the Department of Health and Human Services, and the Department of Veterans Affairs have lots of payment systems that distribute funds based on software systems operating properly.

Student: The other department heads are not in the room for the NSC. How do you fix that? Are they starting to come to your meetings?

Montgomery: I talked about that at lunch. The template now for an NSC meeting—the principal cabinet officers participating—is probably double or triple what the template was ten or twelve years ago.

Student: It's not that way by law.

Montgomery: Actually, it has been changed by a Presidential Decision Directive [PDD].[4] It's nearly doubled. Since the beginning of the Clinton administration, there's been a significant change in the NSC membership. I think at least four or five new agencies, mostly domestic, were added.

Student: What about the other 98 percent of the computer infrastructure? You told us earlier that the government comprises about 2 percent of the infrastructure. What if you'd gone out and put these monitors on, let's say, Oracle (Oracle was here just last week) or Intel or these other large companies to find out how much they're getting hit?

Montgomery: Some companies have done that on their own. The ones who have done it are the banks and the telephone companies: organizations that have high risk of theft. Telephone calling card numbers are about as easy to steal as credit card numbers. In those companies there has been a significant amount of intrusion. We had a telephone company show us their records. It looked like about 5,000 unauthorized intrusions a month. A lot of them are just probes to look for weaknesses, but then you see the same person come back after probing for the weaknesses in automated scans and penetrate the system and remove data. The number of instances of data removal was a lot less than 5,000, but there were still lots of penetrations and removals of data. So, yes, it's happening out in the private sector also, but a lot of industries don't even know it's happening.

Other nations are developing cyber-attack capabilities. Some, even in public discourse, talk about the weaknesses in the United States and the vulnerabilities of our infrastructures to cyber attack. There's a good book out, *Unrestricted War*, which I would recommend.[5] It was written by

---

[4] PDD 2, "Organization of the National Security Council," January 20, 1993.

[5] Qiao Liang and Wang Xiangsui, *Unrestricted War*. As of 1999, only references to this document are available in the United States. See, for example, John Pomfret, "China Ponders New Rules of 'Unrestricted War,'" *The Washington Post*, Aug. 8, 1999, p. A1.

two Chinese colonels, and it details at least one country's evaluation of the vulnerabilities of the United States. It's pretty well written. In fact, it's such a good book that I think it's now being touted as fiction by the Chinese government. But one man's fiction is another man's national security strategy.

I think I've already discussed how cyber war could cause severe damage. It's important to note that it couldn't cause severe damage in countries that don't have developed infrastructures. However, that list of countries without developed infrastructures is getting smaller and smaller.

One of the things that we found during Y2K was that there were significant levels of infrastructure automation worldwide. I don't think it's happening a lot in Africa, other than in South Africa, but I think that throughout East Asia, South Asia, Europe, and even Latin America, there's significant automation of infrastructure. When companies are brought in to build electrical power systems and oil or natural gas extraction systems, one of the requirements of those contracts is that they be heavily automated. Companies are actually requiring that to be built in. That lowers the number of technically trained people that you need to keep on hand, particularly in remote locations.

Privately, corporate leaders do acknowledge the threat when we discuss it with them. They are still reticent about going on the record as saying "My company's vulnerable," because they want to be sure that everybody else in their business sector says the same thing and they all say it together: "*Our companies* are vulnerable." Then they'll feel a little better. Until they're required to do that, I think we will continue to have trouble.

I'll give you an analogy here with Y2K. Most companies were very reticent about saying they had culpability or liability for this, and most CEOs were ignoring it until their general counsels came to them and said, "Here's our liability statement and the extra insurance rider I'm going to have to take out on you personally for Y2K."

Oettinger: Can you explain something that remains a deep puzzle for me? Why isn't the insurance industry not playing a stronger role in this?

Montgomery: Actually, one of the reasons John Tritak's not here is that he is running a White House Conference organized with the insurance companies and auditors. They are beginning to play a role. Their problem is that they were wrapped up in Y2K, and now that they're finished with Y2K they realized that they were going to play just as big a role in the cyber security debate. Audit and insurance companies are going to be the stick that gets the private sector moving. They're going to be the ones that do the analysis that you two talked about, of "When is it required that you make this *x* amount of security effort to defray *y* amount of costs?"

Student: The insurance companies have been hit the hardest with the fraud business.

Montgomery: Yes. The credit card fraud goes directly to the insurance companies…when the credit card companies report it. When they only report 10 or 20 percent to law enforcement, I'm not sure how much they report to their insurance companies.

I just talked about all these different groups (**Figure 3**). I would add that with a terrorist organization, one way you could look at infrastructure attacks is as a physical attack: a bomb against a public switch or against a transformer or substation. I don't think you see that nearly as

much with hackers and criminals. You don't make money as a criminal when you blow things up, not nearly as much as when you steal things. The same goes for hackers and foreign espionage.

Just to recap the implications of cyber threats on national security, one of the things that concerns us is when you read U.S. government planning documents that seem to imply that information superiority or information dominance is a U.S. birthright (**Figure 4**). It's not.

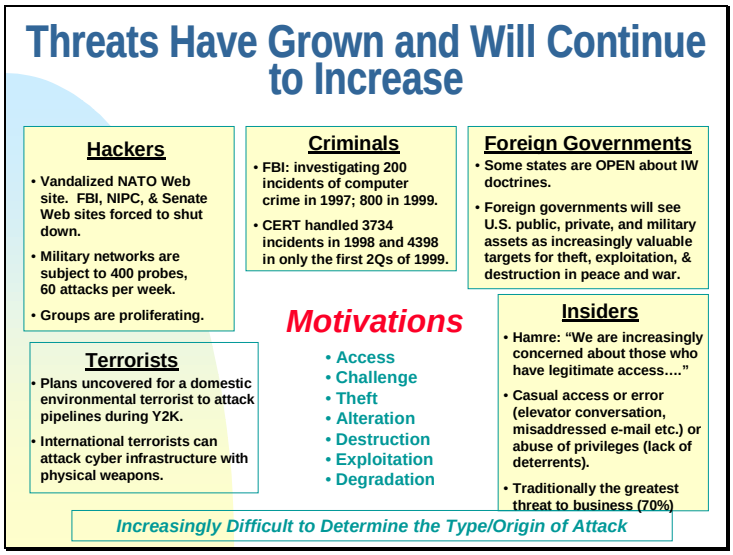

Figure 3

Figure 4

Historically, if you were a "generation" ahead of another country in shipbuilding or aircraft development, it would take them decades to catch up, with significant investments of money and research scientists. With cyber weapons, this going to change significantly. In information superiority, the speed with which your cyber weapons can be matched and passed is mind boggling—and it will require a lot less money and fewer scientists.

This same IT revolution is really shattering a lot of economic development models as well. One of the reasons why I think groups like the IMF [International Monetary Fund] and the World Bank have a lot of trouble properly regulating these economies is their inability to understand this. That's an issue we're just now starting to take a look at. There's a good piece in the *New Republic* this week by Joseph Stiglitz, former head of the Council of Economic Advisors for President Clinton, on the difficulty that some of these organizations have in evaluating that.[6] Right now, the United States has orders of magnitude more to lose in an information attack than anyone else. We are the most infrastructure-dependent economy, and the most infrastructure-dependent national security–military organization. There is a group of countries—Japan, the U.K., and a few others—that have developed (and vulnerable) infrastructures, but they are an order of magnitude less vulnerable than we are right now.

Student: There are voices out there saying that that this is basically a cost of doing business. For example, Wal-Mart has a huge inventory, and about .01 percent of that's going to be obsolete or the employees are going to steal it and all that. After a while, the company just says, "Maybe it's not worth the hassle of trying to prevent that from happening. Let it happen."

Montgomery: You're right. In a retail company, I'd accept that, which is why we have trouble selling the cyber security issue to e-commerce companies. They're generally retailers. That's not true for electric power companies. Pepco [Potomac Electric Power Company] is supposed to provide power, and 99.995 percent of the time it does and .005 percent of the time it doesn't. Usually it's a storm that rolled through town: an act of nature or an act of God. That is accepted. However, they're not expected to have electrical power go down because they have improper computer security and a hacker took them down. What it's going to take, though, to have Pepco motivated is having a hacker take down a similar company, such as PG&E [Pacific Gas and Electric] or Southern California Edison. (I'm not singling out Pepco; their computer security program is not especially weak.) It's going to take a significant cyber security-related failure in the electrical power grid for the companies to acknowledge the threat. The tolerance level is tied directly to the physical experience of the industry. That's why, as you will hear when I talk in a few minutes about ISACs [Information Sharing and Analysis Centers], banking and finance and telecommunications are the industries that have already started to come together on this.

Student: On the first point that you made, I didn't quite get what you were saying about the IMF and the World Bank. Is it that they don't understand the infrastructures?

Montgomery: That's right. I think that if you look at what happened in East Asia in 1996, one issue is that they were not fully capable of understanding the speed with which these countries were able to develop infrastructures. The best example was Thailand, where they were unable to understand the depth of the infrastructure and the economy that developed rapidly through computer systems. In other words, it wasn't the normal "build roads: build telecommunications, build a factory," where it takes seven, eight, ten, or twelve years to build an infrastructure in a local area. You can now build an infrastructure for a high-tech IT-based economy in a year and a half. That's certainly not the only problem. The *New Republic* article doesn't even discuss this, but it discusses a lot of the problems that the IMF and the World Bank were having in evaluating

[6]Joseph Stiglitz, "What I Learned at the World Economic Crisis," *The New Republic* (April 17, 2000), [On-line]. URL: http://www.thenewrepublic.com/041700/stiglitz041700.html (Accessed on March 3, 2001.)

these economies, and then the author argues that, in fact, they evaluated them improperly and created a two-year crisis out of a two-month crisis.

My initial point here was that sometimes I find U.S. defense writings focus on the idea that we're going to maintain information superiority for years and years, as we have with fighters and warships. I don't think that's the case. This is a type of weapon that other countries are going to develop just as fast as we are.

I've already talked about how the public and private infrastructures have become indistinguishable. A good example is that somewhere between 90 and 95 percent of all DOD communications travel on privately owned and operated lines. Almost all of our defense logistics communications are on unclassified, privately owned and operated lines. Clearly, there is a window of vulnerability there for DOD.

I think it's true to say that the U.S. military likes to focus on foreign operations and overseas issues. It doesn't like to concentrate on domestic, homeland protection. Despite this, there has been a lot of attention recently surrounding the establishment of the Joint Task Force for Civil Support for the domestic homeland. It was set up about nine months ago. Unfortunately, its size belies the DOD's commitment to the issue: it's around forty people, men and women. This is not U.S. Space Command's 12,000 or U.S. European Command's 100,000.

Oettinger: But, in fairness to the military, when they have tried on their own to get into this kind of game or have succumbed to civilian inducements, they got soundly rapped on the knuckles. I'm puzzled by hearing you, as a Navy officer, take the services to task on something like this. The last time they tried that I'm aware of was the kind of thing talked about in the Church Committee reports and COINTELPRO.[7] My guess is that folks with long memories will say, "Over my dead body. I don't want to get mixed up with that kind of crap again and take the rap for it."

Student: Look at the blowup we're in over the possibility that one Special Forces person might have assisted the Bureau of Alcohol, Tobacco, and Firearms when they did their takedown at the Koresh compound. It's a national crisis that they sent the military in.

Oettinger: Your statement implies that when you think about this problem and its implications, it's somehow their failing.

Montgomery: I stand by that. I will go along with you that the failure to engage the military fully in homeland defense issues is also the DOD civilians' failing and the White House's failing and the Department of Justice's failing, but "We're not the only people who are unwilling to confront this problem" is not a good argument. Not only the uniformed services, but also DOD civilians, need to think about involving the military. I believe that WMD and homeland defense protection will eventually require the military to participate. I think that's going to open the door for military participation in homeland defense against cyber threats.

Student: Then you get General Shalikashvili's response when he was asked how he would do consequence management: "I'd get a phone book out." His command and control structure is the phone book, and that's pretty scary.

---

[7]The FBI instituted COINTELPRO (acronym for "Counterintelligence Program") in the 1960s to target "radical" political opposition in the United States.

Montgomery: Because we have not been willing to address it, we don't have sufficient processes to respond at all. It may turn out that forty people are enough. Maybe all you need is the structure that says, "We have the list of all the local emergency response systems that we previously trained on this." In addition to the forty people, we are trying to develop seventeen National Guard units that will help respond to biological and chemical incidents. We can't even provide that assistance right now. In the cyber arena, we have no idea which local emergency response systems are well trained to handle a biological incident. We don't have an idea of how many good computer emergency response teams are out there.

Student: As you can see, the whole thing is a mindset. It's a culture thing more than anything else. Once you break that barrier, as Dr. Oettinger was talking about earlier, it will become part of the way we do business.

Montgomery: I agree that the uniformed services are not going to lead the charge here. Someone else is going to have to do that. I'll go along with that, but I don't want to accept what I'm afraid is the next step, which is that, in the absence of good leadership by the uniformed services, no one else will do it. That has been known to happen at the Pentagon.

Student: We had a reading a couple of weeks ago by Gregory Rattray, from the U.S. Air Force.[8] Rattray stopped just short of saying that we need a sort of U.S. Information Force. He drew an analogy between the Air Force being created to deal with a specific new medium of combat, that being air, and today's new medium of combat, the Internet or the cyber world. I thought that Rattray's argument was trying to point you to saying, "We need to stand up a new information force." Is that what you're saying?

Montgomery: No. I'll talk about what I think in relation to that in a few minutes.

Here is another issue (**Figure 5**). This is just getting back to the law enforcement versus national security issue. How do we handle an incident when it first happens? First of all, the first day or two we don't even know it's an incident. It's a computer failure. It's "Your people aren't trained properly." How do we handle an incident when it does become clear that it's "something" malicious, but we don't know if it's a crime or if it's an attack? There are two paths to follow.

[8]Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001).

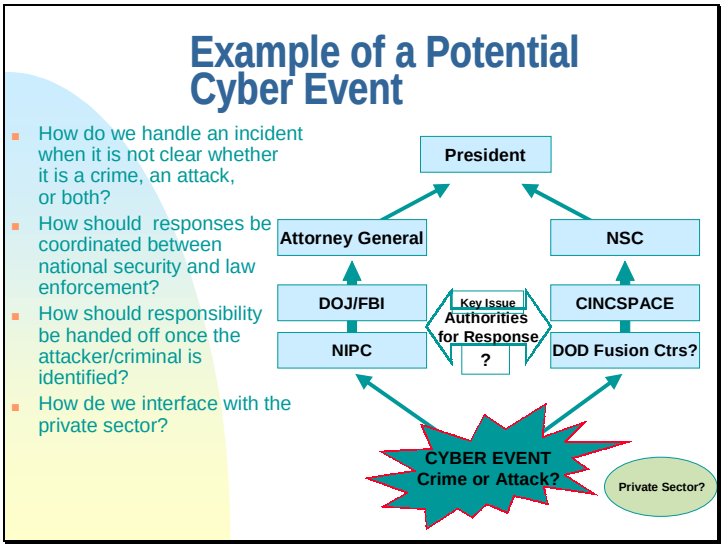

Figure 5

On the first path, the minute it goes to the NIPC [National Infrastructure Protection Center] and law enforcement, information flow to the DOD and the intelligence community stops. We're certainly not going to get it from the FBI because they're going to follow the Department of Justice guidelines and not share that information. So, you have this divergence, and it happens early. If you have chosen the wrong path, you are in trouble.

Where did we see this before? In the investigation of TWA Flight 800 and how we dealt with that. Is it FBI? Is it DOD? Is it counterterrorism? It went with the FBI, and a significant amount of important information that might have shortened the scope of the investigation took a long time to travel between organizations. It slows down the process.

If we do decide it is a crime, it goes to NIPC, which reports to the Department of Justice, and the attorney general then reports to the president. If it goes through DOD it goes through the commander in chief of U.S. Space Command to the NCA [the National Command Authority] and over to the president.

Oettinger: I can't let you get away with saying that it's only the civilian agencies that won't give somebody the time of day. When I was working for the President's Foreign Intelligence Advisory Board, I was sent over to the Joint Chiefs. Jack Vessey was the chairman, and George Joulwan, who later became the commander in chief in Bosnia, was his exec. George threw me out with the words, "Why should we give operational information to some intel weenie from the White House?" So, it cuts both ways, and DOD shouldn't be so holy.

Montgomery: Yes, I am sure that it goes both ways.

Student: I also would say that there is a way to control civilian agencies firmly. You're right: in the military, you direct somebody to do it, and if he doesn't do it you fire him. Civilian agencies, though, can be controlled with their budgets very effectively.

Montgomery: We'll talk about that, as in the Y2K mode.

Student: You were saying the NSC has been changed by presidential directive. Why didn't they go as far as to start holding them accountable, as, for example, Goldwater–Nichols did within the DOD?

Montgomery: NSC accountability is different from that of federal agencies. Membership on the NSC does not put the NSC staff in charge of federal agencies. In federal agencies, theoretically, there is accountability. I'm just saying I don't see it carried out frequently, even for Y2K. If we had not set up John Koskinen to run federal Y2K preparations,[9] with his own budget and centralized government response, the only large agency that would have been ready for Y2K would have been DOD, and they would have gotten ready because they had good centralized control. Without Mr. Koskinen it wouldn't have been as successful as it was. The other agencies were assisted greatly by the central management infrastructure and impetus and because the money was taxed. All budgets were taxed and the money put in Mr. Koskinen's pot, and he would distribute it back to each agency. The agency had to go to him with its remediation plans to get the money, and, amazingly, the agencies would become very cooperative and comply with his high standards. He provided us with centralized control. If we could have kept him on in charge of information security, we'd have great information.

Student: Get hold of money.

Montgomery: Before I get into what our solution was, these are the kinds of indicators of cyber vulnerability we watch (**Figure 6**). As I said before, a lot of people tend to think information superiority is some kind of U.S. birthright, but this is belied by the fact that the patent diffusion rate is spreading significantly. More and more software development is being done outside the United States. There is a shift in the software production market. Today, 80 percent of software producers are either in the United States or U.S. companies on foreign soil, but the movement overseas is increasing. There's also a change in the education and skill mix. The lack of software development curricula, particularly in cyber security, is shocking in the current environment, and the number of U.S. students majoring in computer science is actually going down. From 1986 to1996, the number of people studying for bachelor's or master's degrees in computer science went from 50,000 to 35,000. The proportion that were non-U.S. citizens went up, so the number of U.S. citizens doing this really went down.

[9]John Koskinen chaired the President's Council on Year 2000 Conversion, 1998–2000.

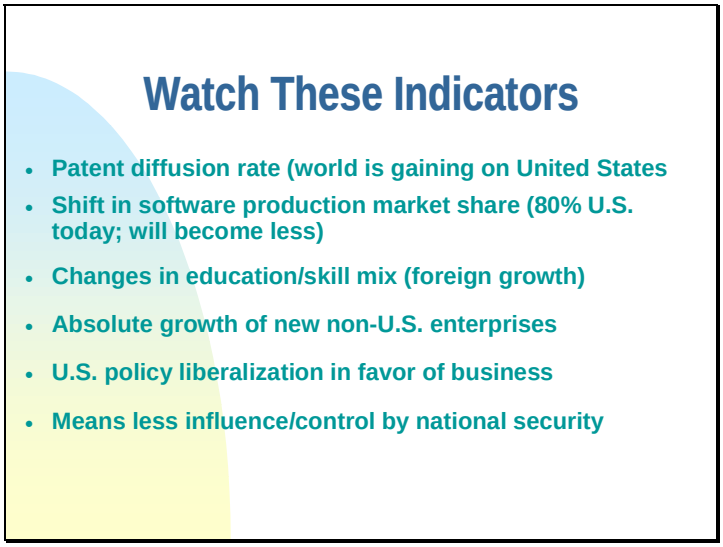

Figure 6

Student: I hear educators complaining constantly that students are bailing out of the social sciences and going into the computer sciences because that's where the money is. It's a common lament over in Harvard Yard.

Oettinger: I'm in Arts and Sciences.[10]

Montgomery: As a postgraduate history student who is now a nuclear engineer, I've done both sides. I can tell you that it's a lot harder to stay disciplined and get the engineering work done. That's my opinion.

The H-1B visa program validates this. Companies are lobbying their senators to get them to increase the allowable quota. It has gone from 25,000 to 115,000 a year. I love that system, because I think that brings in up to 115,000 people in IT who may eventually become new U.S. citizens. Obviously the unions have a slightly different take on it than I do, but I think the H-1B visa program is a success. It may be nationalistic of me, but I think six years in the United States generally have a very positive effect on people's perception of the United States and their likelihood of becoming U.S. citizens.

Student: Over 60 percent of the Chinese who study over here become citizens.

Montgomery: That's a great thing for us. We ought to raise it to 200,000 H-1B visas.

One of the things that's really interesting, and I discussed this earlier, is that economic issues, business issues, are more and more becoming driving factors for the NSC. They're no longer an aside, like "Oh, by the way, this will help a U.S. industry."

So, what happened in the United States? Stepping back for a second, a computer security revolution was occurring throughout the 1980s, and individual scientists knew that there were security flaws. It really wasn't until 1990 that we had a national-level report, when the National

[10]Anthony G. Oettinger is Gordon McKay Professor of Applied Mathematics, Professor of Information Resources Policy, and a member of the Faculty of Government, part of the Faculty of Arts and Sciences, at Harvard University.

Research Council, which is part of the National Academy of Sciences, a very well-respected organization, put out *Computers at Risk*.[11] There were lots of meetings and things like that, but no national strategy really developed out of that. By the way, this doesn't deal with DOD.

Around this same time, in the late 1980s, DOD recognized that computer security and computer information systems were a significant issue. There was a lot of vision at the DOD, particularly among Air Force officers, and it resulted in the establishment of some information systems commands like AFIWC [Air Force Information Warfare Center]. That was happening in the background at DOD.

In 1995 there was an act of domestic terrorism: an American citizen blew up the Murrah Building in Oklahoma City. As a result, the federal government formed the Critical Infrastructure Working Group under Attorney General [Janet] Reno. One of the first things this group realized was that information security in itself is a massive issue. Senator [Jon] Kyl [R-Ariz.] was receiving some of these same briefings, and he added money to DOD's budget to look at these kinds of issues on a national level. One of the outcomes was that the Presidential Commission on Critical Infrastructure Protection [PCCIP] was formed. I think you have books on that.

Oettinger: Michelle Van Cleave's presentation from last year gives background on the Kyl Amendment,[12] and there was also the Rockefeller report, which was mentioned previously.

Montgomery: Other things are missing from this slide [Fig. 6]. As I said before, a lot of blue ribbon panels meet every year, and probably ten or twelve nice blue ribbon panels arrive in our office alone on different counterterrorism issues. When the report of the PCCIP came out in October 1997,[13] things happened. It was an important issue. Only seven months later, in May 1998, a PDD was issued: PDD 63, which you have looked at as well.[14]

What was the goal in PDD 63? It was not to prevent all cyber attacks; although we sometimes write seemingly unachievable goals into government documents, this was not one of them (**Figure 7**). The goal of PDD 63 was to prevent or mitigate attacks. The reality is that attacks will occur. The first thing you should do when a computer software guy comes to you and says, "I have the magic bullet here. I've checked all your systems. My new software defeats every known attack," is fire that contractor because he is selling you a line. There is no magic bullet, and there will never be a magic bullet. As long as there are people involved in the system, as long as there is new software being issued, there is no magic bullet to ensure cyber security. Software that Microsoft issued only five months ago already has several hundred known security deficiencies pointed out, most of which Microsoft has acknowledged and already issued patches

---

[11]National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, D.C.: National Academy Press, 1990).

[12]See Michelle K. Van Cleave, "Infrastructure Protection and Assurance," in *Seminar on Intelligence, Command and Control, Guest Presentations, Spring 1999* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-00-2, June 2000), [On-line]. URL: http://www.pirp.harvard.edu/pubs.html

[13]*Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection* (Washington, D.C.: The White House, October 1997), [On-line]. URL: http://www.ciao.gov/PCCIP/PCCIP_report.pdf

[14]*Protecting America's Critical Infrastructures: PDD 63* (Washington, D.C.: The White House, May 22, 1998), fact sheet [On-line]. URL: http:www.fas.org/irp/offdocs/pdd-63.htm

or repairs for. Our goal is to prevent as much as possible, and, then, equally important, mitigate the effects of those attacks that get through.

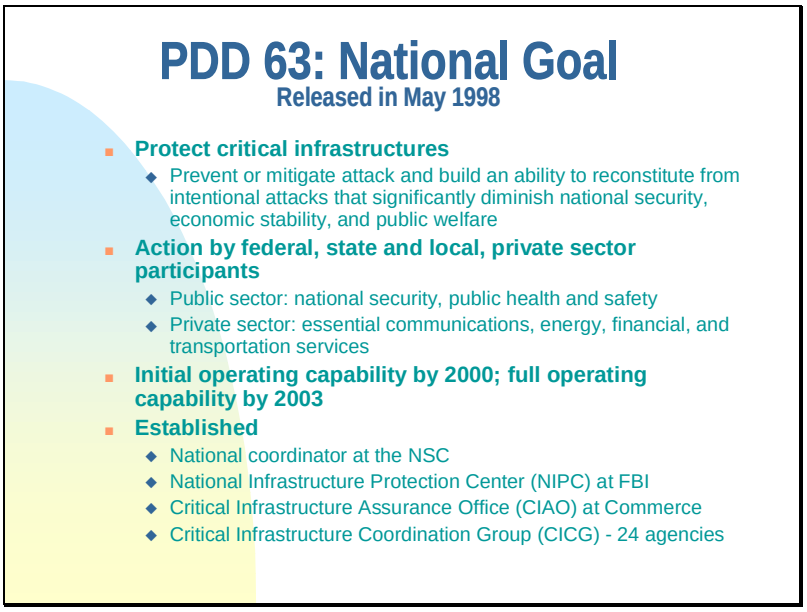

Figure 7

The best way to mitigate cyber attacks is to build a reconstitution capability to respond to cyber attacks that would otherwise diminish our national security and stability. The reality is no one cares that commercial companies such as eBay or E*TRADE or Amazon are shut down for two or three seconds or two or three minutes. That happens every day anyway. It happens because of personnel errors or software errors. What people care about, what spurs the Associated Press to write a story, and why we have a presidential meeting at the White House, is when commercial sites are shut down for two or three hours, or two or three days, or two or three weeks. Cyber reconstitution is the ability to absorb a blow and rapidly reestablish our systems. Absorbing a blow may mean absorbing it into a "honey pot" of replicated information systems so you'd never even experience a real attack, or reconstitution may mean the ability to be totally knocked down and have a redundant system or the same system restart back up rapidly. In my opinion, reconstitution is the key to success in this issue.

Overall, we recognized that protecting our critical infrastructure was no longer a federal issue. As I said, it isn't DOD anymore, and it isn't law enforcement: it's all of the public sector and, most important, the private sector. The PDD also directed that we build an initial operating capability [IOC] by 2000 and build a full operating capability by 2003. I know you only read the "white paper" version of PDD 63. I can tell you that in the actual version of the PDD it doesn't describe initial or full operating capability either. That was probably good and bad. It was good in the sense that it didn't pin us down, because we've been on a steep learning curve over the last two years. If you're pinned down by a PDD that gives you direct guidance, it's hard to change when it's bad. So the good news is it was pretty vague.

It is still difficult to identify what constitutes an initial operating capability. I think it's probably "have enough initiatives in play that you're beginning to address the personnel,

technology, and standards issues." What's full operating capability? I don't know, and I certainly don't think that anyone can tell you very accurately today what the computer security environment is going to look like in 2003. The PDD certainly couldn't in May 1998.

PDD 63 also set up some working relationships. It established my boss, Dick Clarke, as the national coordinator in the NSC. We tried to mirror the arrangement we had built for counter-terrorism. Having worked for Mr. Clarke under both of his hats, the directive power that the national coordinator has in counterterrorism is far different from and more effective than the coordinating power he has in critical infrastructure. It's probably because we still respond to incidents involving physical terrorism as crises. Things involving critical infrastructure are more process, and we still treat them very differently, with less central control.

The PDD established the NIPC at the FBI. It's an interagency group: mostly FBI, DOD, and intelligence community personnel, and some local police people to handle the law enforcement and the intelligence issues associated with critical infrastructure and cyber crime. It also set up the Critical Infrastructure Assurance Office [CIAO], John Tritak's office, and assigned it the roles of conducting private sector outreach and helping Mr. Clarke organize the federal government's cyber security efforts. Finally, the PDD established the Critical Infrastructure Coordination Group [CICG]. This NSC-led group has 24 agencies represented. When we convene this group sometimes, the only thing you can agree on is that the meeting ought to end in an hour and a half. It is difficult to organize so many disparate agencies. For the sake of comparison, WMD is about a twelve-agency group and most of the national security issues are about four to eight agencies, so you can see the problem with the CICG having twenty-four agencies.

The PDD also directed us to "Come up with a national plan to develop your initial operating capabilities." We released that in January 2000 (**Figure 8**). You have seen the plan, and it has about ten major programs in it. I really try to break it down to just ten issues. I should know, because I've fought tooth and nail to make it a number I can remember.

I try to break those ten programs down to three general areas. The first is standards, which is the effort to improve the standards that we establish for computer security in the government. Let me say that the goals of the national plan—making the U.S. government a model and building a public-private partnership—are broad. By contrast, establishing standards that identify and

Figure 8

address vulnerabilities and making departments develop critical infrastructure plans are very specific programs. Evaluating standards enables federal agencies to realize they have vital computer systems and then to build an expert review team that will assess their efforts and do "red teaming." The NSA will help to do this red teaming for the DOD: assess critical infrastructure and fix the security, and draw attention if they've fallen short. The proposed expert review team will do the same thing for the non-DOD agencies: help them determine where their weaknesses are and address their vulnerabilities.

Implementing best standards and practices is a proposal that has been out there for a while. It has been part of Clinger–Cohen;[15] it's been part of various computer security initiatives since 1987. We've been preaching the value of establishing standards for years, but we haven't achieved it. Federal agencies are inconsistent in their implementation of best standards and practices, which is usually a function of insufficient budgetary resources being applied.

The second general area is technology, and this includes installing firewalls and intrusion detection systems to detect and block attacks and building a netted and adaptive system, the Federal Government Intrusion Detection System [FIDNET]. FIDNET has received a lot of bad press. It is supposed to do three things. First, it's a way of rapidly installing software patches. Right now, let's say that you own a Microsoft Windows NT system, and Microsoft says, "Dear me, we've found this back door (or some other flaw)." Microsoft is usually the one to detect it, or a security expert tells them about it. They build a software patch, test it, and then release it. They don't say there was flaw *x*, *y*, or *z*. They just say, "Install this patch if you have Windows NT 4.2 or 4.1." So, out it comes, *boom*! Your system administrator is supposed to know how to find the patch, check the site frequently, download the patch, install it, and test it on your system. Rather than have you guess, I'll just tell you that the average amount of time it takes a private sector

[15]The Clinger–Cohen Act of 1996 established the role of CIOs in the government, and set up the interagency Chief Information Officers' Council.

company to do that is sixty to seventy days after Microsoft posts it. The average time for federal agencies is forty-five to fifty days. The average time for DOD is about thirty days.

In the meantime, hackers can download that patch, reverse engineer it, determine the flaw it was designed to correct, develop potential attack scripts for the flaw, and then post the attacks on the Web site. So, from day 1 or day 2 when the attack script is on the Web site until your company installs the patch (sometimes they don't even care), you now have a known entry point where someone can exploit your system. That's a serious flaw. What we want to do is build a system where we can automatically alert people to the flaw, then automatically provide, install, and test that patch.

That type of software is under development, but there is a potential problem with this development effort. Let's say you have a system that automatically alerts you and installs a patch, and I'm a really crafty, skilled hacker. What am I going to do? I'm going to build a patch, or I'm going to grab the Microsoft patch while they're working on it and install another flaw in it so that you automatically install my flaw in your system. You've got to be very careful with that. It's an interesting problem.

The final area, and the one I work on most, is personnel. Being from the military, I really like this issue. It's certainly not easy, but it's challenging. We're developing something called the Federal Cyber Service or "Cyber Corps" program. This is an effort to recruit, train, and retain information technology specialists in the federal government. Yesterday I read that the Information Technology Association of America, a cyber industry lobbying group, reported that in the United States there will be 1.4 million new IT jobs created over the next year and a half. Over the next five years, there will probably be about 50,000 new IT jobs created in the government. But we're not graduating or training nearly enough qualified personnel to fill those jobs. The problem in the government is, if you're Bill Gates without your college degree and you dropped out of Harvard, we can offer you a job as GS-7 at $37,000 a year. That's obviously a lot less than an IT professional can make on the open market. It makes it difficult for us to hire good IT people.

What does that tell us? You don't have to have a college degree from Harvard or from Frostburg State or anywhere to become a skilled IT worker. One of the things we also have to evaluate is why we hire information professionals without college degrees as only GS-7s.

Oettinger: It's a terrible advertisement for this university, because all the dropouts have had a very strong influence not only on the economy, but also on the whole area of intelligence. Another Harvard dropout, Edwin H. Land, was the impetus behind the development of the U-2 program, and eventually the various satellite programs that kind of kept the cold war from getting hot for forty years. So, if you want to have influence on national security and get filthy rich, don't get a degree!

Student: Leave after your junior year. That's the way to go.

Montgomery: We have identified the need to recruit a cadre of people, so we developed the Cyber Corps program, where we plan to give about 300 scholarships a year to students for their junior and senior years or their master's program, and then they will owe service after graduation to the federal government. It's exactly like our military's ROTC [Reserve Officer Training Corps] program. Not surprisingly, because I'm an ROTC graduate, I like the program. We even have

summer training planned where the students will work for a federal agency and try to develop a mentor relationship there to determine if that's the right agency for them to be placed with. Over the year and a half they can also get their security clearances and so forth.

The next thing we need to do is train our current IT workers. We have 75,000 or so IT workers in the government, and half of them weren't formally trained. We need to develop a standardized and approved cyber security curriculum and training program. We're not going to build a unique government training program, first, because we don't have the money for that, and second, because Cisco and MIS and lots of private companies run really good training programs already. So what we have to do is determine what skill sets and competencies we want for each type of IT job in the government, ask "Which one of your courses covers this?" and tweak the course a little because we're a big contract. We'll validate those courses, and then we'll subsidize government workers going through them to get proper formal training.

The final thing is that after we recruit them and train them we've got to retain these IT workers. That's the hardest part, because near D.C., in northern Virginia, there is the Dulles access road, which is full of IT companies.

As an example of our retention problem, an Air Force major from AFIWC comes up to brief us about every three months. A new one comes up three months later, and if I ask where the old one went, he says, "I think he's somewhere in San Jose or northern Virginia." You guys have spoken to someone who as far as I can tell is the only major who ever briefed us and actually stayed in the military service, and that is Greg Rattray. The rest of them get out. In the armed forces we are losing our IT professionals, both officers and enlisted, as fast as they can get out. I went to Microsoft's operations center, and about thirteen out of fifteen guys in there had a military—either Navy or Air Force—logo on their screen saver. They were ex-U.S. military.

The good news there is that the military is pumping great IT workers into the work force. The bad news is we don't have enough people with significant experience doing IT work in the government anymore because they leave. The other good news is that the armed forces seem to be able to recruit their 10,000 new IT workers each year. One place the Navy doesn't have trouble recruiting enlisted guys into is our new IT rating, but I'll bet we'll have a lot of trouble retaining these sailors four or five years from now. We've got to figure out how to pay them more.

Student: I just want to mention that the problem in general goes beyond the military. For example, a lot of lawyers are moving away from practicing law and going into IT.

Montgomery: That's actually some of the best news I've heard today. I'm joking, but you're absolutely right. As I said earlier, 1.4 million new jobs are developing in the U.S. private sector over the next eighteen months. There are actually millions of IT jobs that are empty, or not properly filled, or where one person is doing what a company should pay two people to do. At the managerial level, the pay discrepancy between the public and private sectors is even greater. We have a significant problem in our military and in the federal government.

I also think that in the private sector this will lead to rapid movement of people between companies. Although it is a new phenomenon that is sometimes good in business, it's going to be very tricky when you're responsible for a lot of information systems. If people just move between companies a lot, you're not going to have the kinds of systems expertise and institutional memory you would want.

A separate issue I'll try to expound on is the need for a robust research and development [R&D] program. We were surprised how little money the non-DOD federal agencies and private sector are spending on R&D in computer security. Just two years ago, the government was spending only about $450 million on computer security R&D, of which $410 million was DOD and the intelligence community and $40 million was all the other agencies together. There is a lot of money being spent on R&D in computer and network operating systems, but when it comes to security, there isn't as much money to be made and consequently less R&D money is invested.

I'll give you an example. If you were building the next Windows operating system, and you could build it with almost no security for $100 or with great security for $150, which are you going to do? You're going to build the $100 one because you want to outsell Sun Microsystems' competing $100 system with no security. The lowest bidder will win almost every operating system contract. If you deliver a system that works operationally (not in terms of security) for less than your competitor, you will be chosen. What we've go to do is convince companies to spend the extra $50 on improved security for their software. Microsoft (and their competitors) will make the improved security products if they believe there is a market for them. That's the argument we are trying to make.

This leads into what I was supposed to talk about for most of the class (I'm sorry about that): establishing a public-private partnership to protect our national infrastructures (**Figure 9**). This is where we've got to go out to the private sector and say, "Listen, you own and operate a telecommunications system. You own and operate banking and finance systems. You own and operate natural gas and oil pipelines. You need to build good security into your systems." This is sometimes a very difficult sale. The first thing we try to say is, "Ignore the government. Forget we're even here. Just build computer security centers within your industry so you can share your experiences with each other, because individually you're telling us once in a while about massive pilfering or theft or loss of proprietary data. If you would share it with each other and as a group say, 'We have this problem,' maybe you could sell that to your shareholders as an issue to

Figure 9

deal with. You certainly are not going to do it by saying, ‘Alone we will go out and admit there’s a problem in the credit card field.’” The banking and finance industry was the first to take us up on this. Why? Because they have had the most cyber crime. The financial services ISAC has been set up in Reston, Virginia, and the companies are beginning to share information with each other and cooperate on security system development.

Oettinger: They are more vulnerable to government regulation than anybody else, so they know that good behavior is rewarded.

Montgomery: We went on to recommend to ISACs that “The first thing is that you show each other information on attacks. The second is that you receive threat information from us. If we know of a type of attack or explicit attack, or even a general issue that a criminal group is thinking of, we’ll tell you.” On receiving information from us, they initially turned us down flat. They just don’t want it. The reason they don’t want it is because they don’t want the proposed third element of an ISAC, which is sharing experiences, events, and incidents with the government. Since they don’t want number three, they’re really hesitant to start up number two seriously.

As I said, banking and finance have started working. They’re even looking at pooling R&D money to develop the next level of security software, maybe as a group, specifically for credit card and financial transactions. The second industry that has an ISAC is telecommunications. This was really just recognizing that we already had a phenomenal relationship with the telecommunications industry inside the National Communications System, which is a DOD-sponsored entity. Within that, post the AT&T breakup, all the long-haul carriers came together to share information on network reliability and system readiness. This came at the same time as the National Security Telecommunications Advisory Committee. At the NCS, the companies share threat information, we share threat information with them, they tell us about reliability incidents, and they work together. The telecommunications industry is also regulated, so that the two industries that are really regulated actually have formed these ISACs. The other industries haven’t formed ISACs yet.

The federal government has also set out to develop a broad-based government-industry partnership. That’s where we’ve reached out to the Fortune 500 companies to meet with us and talk with their competitors about computer security and raise awareness. About 150 of the Fortune 500 have signed up, and John Tritak in the CIAO and Secretary [William] Daley of the Commerce Department have been running that effort for the government.

We’ve also proposed a permanent presidential advisory panel. It’s made up of thirty members: ten CEOs from IT companies, ten CEOs from infrastructure companies like banking or oil and gas or electrical power, and ten kind of academic, privacy and state and local government experts. This group of thirty people would come together and serve as the President’s advisory panel on infrastructure assurance issues: the National Infrastructure Assurance Council.

The final thing we’re attempting to do is create an Institute for Information Infrastructure Protection. Neil Lane, the president’s science advisor, and Sandy Berger, the national security advisor, each worked to place about $25 million, to give us a $50 million program. The institute will then look for the gaps between what the DOD is doing for computer security R&D and what the private sector is exploring, and try to fill these gaps.

Someone mentioned earlier the need for software to detect malicious code that was written by a malicious software engineer who wasn't trying to help his company. Under the cover of "upgrading" software, he installed some back doors. We want to develop software that automatically scans your system and alerts you to malicious code. Right now, we have systems that say, "ABC is a bad piece of software code. It's a trap door." So, you run this and anywhere there is ABC, it detects it and says, "I found ABC. Let's go take a look to see if it is a trap door." We need more intelligent software that is able, on its own, to evaluate and recognize that, "Hey, BDA is also bad software. In this context, it's a trap door. We've got to get in there and remove all the software that's written poorly." That's what we're working on now.

In terms of funding, the federal government spent $1.75 billion on cyber security in FY 2000 (**Figure 10**). In FY 1997, we spent $1 billion, and in FY 2001, we have proposed $2 billion. You can see that over three or four years we've doubled the amount of money we're spending on computer security in the government. Although it's an admirable increase, it's still not enough. If I made the call, I'd spend about $3.5 billion on computer security—triple or quadruple the 1997 budget. This $3.5 billion is not happening because domestic spending is actually pretty tight, and that the actual expenditure even doubled tells you how seriously we are taking this.

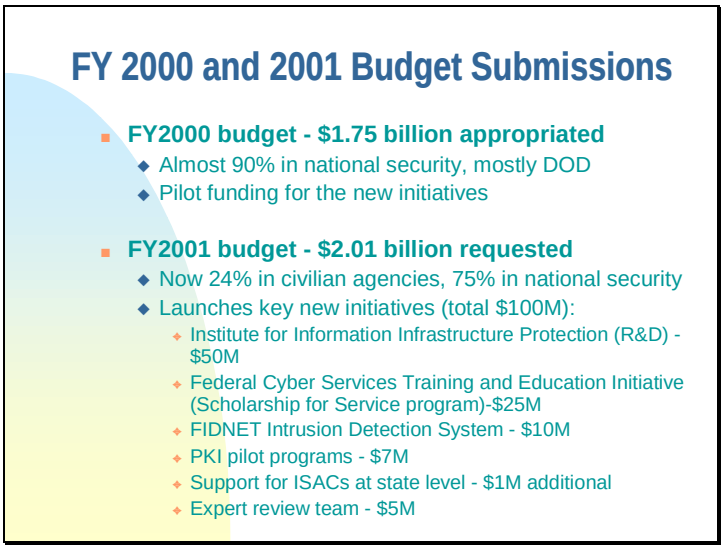

Figure 10

The budget used to be 90 percent national security agencies (DOD and the intelligence community), and we've moved it down to 75 percent. It eventually needs to be 50 percent. Agencies such as Labor, Agriculture, Commerce, and Treasury should be spending as much money (in total) as the DOD and the intelligence community.

We've also launched six new key initiatives tied to the ten programs I mentioned earlier. One is that institute for R&D that I just talked about. Another is the Cyber Corps training program. They get the bulk of the new initiative money.

Then there's our FIDNET program of about $10 million. We're also trying to figure out how we can best use a public key infrastructure [PKI] pilot program, because while it does offer some protection, I do not think that PKI is a silver bullet. Some people treat PKI that way: if I

encrypt and you encrypt and we use common encryption, then no one can break it. That's not true. NSA can break many PKI programs, and I assume foreign intelligence agencies can do the same. I'll go one further and assume some private hacking or computer investigative groups can do it as well.

We're also putting small initiatives in for supporting ISACs and building an expert review team to red team our federal systems. There is still not enough money. Frequently, when we brief on the Hill, they essentially say, "Great, but you're late and you're not spending enough." That's music to my ears.

I'll just talk a little bit about what the DOD was up to (**Figure 11**). It's not germane to our overall topic, but I would say that the DOD and the intelligence community got ahead on this issue ten or twelve years ago and that's why they're in much better shape.

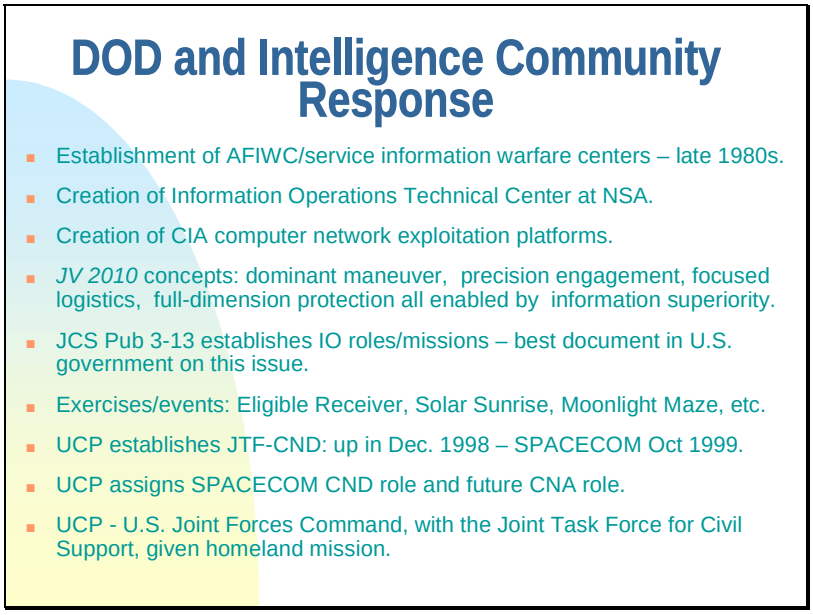

Figure 11

That was my show there. It wasn't a big bang of an ending, but that's the way I look at it. I've got a few more minutes to answer questions if anyone has any.

Student: What are the standards for initial operating capability for PDD 63?

Montgomery: I was afraid someone might ask that. As I said earlier, we don't have them. One of the reasons they're not written down is that we didn't want to find ourselves tied to those same standards three or five years later. Initial operating capability, we determined, was identifying problems and developing initiatives to correct them—specifically, improving our standards, our technologies, and our personnel situation. More accurately, we are defining an initial operating condition; it's not a capability.

The concept of final operating capability is the ability to defend against and prevent most cyber attacks and build a reconstitution capability to mitigate the effects of successful cyber attacks—to rebuild from an attack. I haven't shown you a single budget dollar for reconstitution, and I'll tell you why. As a government, we don't have a good handle on how to conduct

reconstitution yet. We don't know how to reconstitute local power if Pepco were successfully attacked. Is it proper for the federal government to pump millions of dollars into new software systems to get the company working again? Is it proper for the federal government to order Pepco to have a backup transformer at every station or to have backup public switches? Is it proper for us to provide a tax incentive for Pepco to build those, or should we just let the attacks happen and let Pepco's customers and shareholders lose confidence and then push the company to build a reconstitution capability on its own after an attack?

Those are challenging questions. They are hard to answer, and our efforts to deal with them are so basic that you won't even find them addressed in the national plan, because we couldn't have gotten interagency agreement on how to do that. One of the most promising ideas is for the Office of Management and Budget to provide a tax incentive for companies that invest in reconstitution capability, which is probably the fastest way to get things done. DOD had a program, the Strategic Sealift Reserve, under which shipping companies would get funding from the U.S. government when they built a cargo ship. The deal was that in wartime the cargo ship would revert to the U.S. government for sealift. That was a successful incentive program. Theoretically, that's the same kind of national security infrastructure program we ought to have for the electrical power industry or telecommunications industry so that they build a capability to reconstitute rapidly in a national emergency. This remains a difficult issue, and I don't think we'll have final operating capability until we figure out how to solve reconstitution.

Student: You mentioned earlier that you were open for development of an artificial intelligence program that would read code and understand if code was not sufficiently strong to keep an attacker out. I remember when SATAN [Security Administrator Tool for Analyzing Networks] came out. SATAN was developed as a means for people to go around evaluating systems, but, of course, as soon as it came out the hackers grabbed it and started using SATAN to launch their attacks. They scanned other systems to find vulnerabilities. If you develop this artificial intelligence code, how are you going to keep it from becoming the hacker's best weapon for penetrating your systems?

Montgomery: Let me explain the artificial intelligence program a little better. What I meant to say was it's a system that detects back doors or other malicious software code and therefore lets you know of your vulnerabilities.

Student: That is what SATAN does. It scans your computer and looks for vulnerabilities.

Montgomery: You're right; that could be a problem. My answer would be that you should inspect SATAN and use it first, and then prepare your patches. I can't give you a silver bullet answer to that one.

Student: How is infrastructure dealt with on different levels? Could you compare the United States on a national level with the international level? Are those international concerns about IT stuff basically centered in the IMF and the World Bank?

Montgomery: That's a good question. No, it's not at all. The World Bank and IMF probably ought to be cognizant of infrastructure vulnerability issues.

You have raised an issue I said I would address, so I'll mention it here. We are examining international efforts on IT security and global information infrastructure evaluation. Currently, we are concentrating on the criminal aspect. In other words, maybe we all can get together and agree

what constitutes cyber criminal behavior, or how we will exchange information rapidly with each other to chase down a hacker. Just getting countries to have a cyber crime duty officer twenty-four hours a day, seven days a week, would be a help. Many of them don't have operating centers to respond to cyber crime. There is no one in these countries one can contact and say, "We're being hacked from Nairobi University. What are you guys doing to stop this?" In many countries, there is no one we know to call who works on this issue. We have the NIPC, but we've only had that capability ourselves for about a year and a half. We are not looking at this as an international issue in enough depth…probably to our long-term detriment.

Oettinger: Could you pursue that a little bit further? Speculate on what is sort of a favorite question of mine, which is explaining why all sorts of things don't happen that one might imagine would happen. They don't happen for different reasons. Why haven't the world's major water supplies been poisoned as a tool or weapon of mass destruction? One of the reasons is that it turns out that if you want to poison the whole water supply, it takes an enormous amount of poison, so it would require a major operation and your ordinary terrorist can't quite pull it off. Another reason was triggered by what you were just saying. After an initial spate of airline hijackings and so on getting more and more frequent, folks got together, even with Cuba, so that there is a sense that we will stop it because all of us are losers in this. Those things stabilized and the rate of hijackings slowed down. It was not totally eliminated, but it's better than it was in the early days. Your example then of maybe getting together with some countries that have warning centers and so on is one example of arranging things to increase the probability of nothing happening. Could you explore this a little bit more? What are we doing to assure that nothing happens?

Montgomery: Probably not enough. We are working with the G-8. We are the biggest source of computer crime, and I would say most cyber criminal activity passes through the G-8 countries and China. Those are probably the final ISPs through which the hacker ends up going.

At the Council of Europe, where we're actually an observer, we're working closely to try to get a cyber crime treaty that would extend beyond the Council of Europe and would have lots of signatories. Essentially what we're attempting to establish is the definition of what a computer crime is, how we will share information on criminal activity, how we will cooperate, and how we are going to do a hot pursuit in cyberspace, because that's a big issue. You could be following somebody along and the next thing you know, you've just ended up in a Canadian university and then a Chinese university and then a German university (I picked universities because they have some of the weakest computer security). It's very easy to violate sovereignty issues.

So I'd say those are our two biggest efforts. We'll see how they go. I think the Council of Europe initiative has a good chance of being a treaty. The G-8 will be a combined policy effort. The countries that have the biggest infrastructures are going to start imposing some kind of cyber monitoring system internally and start to create an international code of cyber law.

Student: I think the agreement is that there is no nationality on the Internet.

Montgomery: I don't think that will be included in the agreement. I wouldn't agree to that concept. The U.S. certainly won't. I also believe that every country that has a good, well-developed ISP system—China, the United States, Russia, and Germany—wouldn't agree to that.

Student: If you had an international agreement and the national agreement was subservient to the international agreement.…

Montgomery: Yes, but countries first have to sign on, and as I said, they won't.

Oettinger: They won't sign on for national security reasons until all the infinite set of taxation issues have been resolved.

Montgomery: That's probably utopia. At least the way I look at things right now, that will not happen. That's my opinion.

Student: Are they looking at tying those together—that is, tying international taxation rules and so forth together with information sharing about crimes or terrorism? One is kind of an incentive, and the other is kind of a cost.

Montgomery: Not that I'm aware of, only because the only way you would avoid a national tax is if you were selling an idea. Most things that you buy through the Internet still get shipped. They have a customs duty attached to them.

Student: Except for CDs and films.

Montgomery: That's a fact we're hitting on where there's been the most need, but also the greatest friction, because the intellectual property issues associated with cyber crime are significant. You were talking earlier about lawyers leaving for the IT world; I also see a lot of lawyers getting training on intellectual property and IT and putting up a shingle. I'll tell you, you're going to be a rich lawyer with that background, because that is going to be a growth issue over the next few years. I think it is going to be the breaking point for some countries. It's going to be a significant issue for some countries and the WTO.

Oettinger: His advice is: go to law school.

Student: It seems that part of the problem you have identified here is trying to get an international standard of security established. When we think about the other international standards that are widely accepted, there is the Uniform Commercial Code, or generally agreed accounting principles, or Windows. All of these international standards are adopted because it is in the personal economic interest of each individual to adopt it. In the case of generally agreed accounting principles, you cannot go public with a company on any major stock exchange unless you do your books this way. It's the same thing with the Uniform Commercial Code; you can't do business unless you meet that. Of course, it's obvious why you would adopt Windows or a standard operating system. How are you looking at making it economically to the advantage of each individual, rather than trying to impose these standards from the top down through governments, which I don't see succeeding?

Montgomery: What we are looking for from governments is purely law enforcement. You're absolutely right. For standards, it's going to have to come from groups such as the auditing and insurance companies. It's going to have to be the private sector that leads this effort; the government can't. You're absolutely right. It's the same with encryption. We tried to impose our will with it for a while, but I think that in the end the private sector will drive it.

There is one thing I said I was going to touch on and that is Y2K. One of the great things we did for Y2K was that we organized our federal government with an assistant to the president, John Koskinen. He got his own budget, and he worked with a special committee in the Senate that was set up under Senator [Bob] Bennett [R.-Utah] and Senator [Christopher] Dodd [D.-

Conn.]. It was a great system. I stated earlier at lunch that we got through Y2K, and it was probably the greatest managerial and technological challenge that has faced our country since World War II. It was not about leadership of the country, or making tactical battle decisions, but how to get through this. It was a $600 billion effort worldwide: $300 billion in the United States. That's a lot of money. That's serious dough. You'd need three fortunes the size of Bill Gates's to do it. Unfortunately, once we completed this task people inside our government immediately weakened and disestablished the centralized IT team that managed Y2K, so we cannot apply it to these challenging cyber security issues.

Oettinger: A small token of our large appreciation for you.

Montgomery: Thank you very much, sir.

Acronyms

AFIWC	Air Force Information Warfare Center
ARPA	Advanced Research Projects Agency
CEO	chief executive officer
CIAO	Critical Infrastructure Assurance Office
CICG	Critical Infrastructure Coordination Group
CIO	chief information officer
CNA	computer network attack
CND	computer network defense
DISA	Defense Information Systems Agency
DOD	Department of Defense
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FIDNET	Federal Intrusion Detection Network
IMF	International Monetary Fund
IO	information operations
IOC	initial operating capability
ISAC	Information Sharing and Analysis Center
ISP	Internet service provider
IT	information technology
NIPC	National Infrastructure Protection Center
NSA	National Security Agency
NSC	National Security Council
PCCIP	President’s Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PKI	public key infrastructure
R&D	research and development
ROTC	Reserve Officer Training Corps
SATAN	Security Administrator Tool for Analyzing Networks
UCP	unified command plan
WMD	weapons of mass destruction
Y2K	year 2000

INCSEMINAR2000

ISBN 1-879716-74-7