INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Securing Cyberspace
Gregory J. Rattray

Guest Presentations, Spring 2004
Carol A. Haave, Mark M. Lowenthal, Robert B. Murrett, John C. Gannon, Joan A. Dempsey, Gregory J. Rattray, Robert Liscouski, Arthur K. Cebrowski, Aris Pappas

January 2005

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN I-879716-89-5 **I-04-1**

January 2005

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Ltd.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Strategy Assistance Services
TOR LLC
TransMedia Exchange
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

Verizon

Securing Cyberspace

Gregory J. Rattray

April 15, 2004

Colonel (select) Gregory J. Rattray, USAF, is director for cyberspace security on the National Security Council (NSC) staff. Previously, he commanded the 23rd Information Operations Squadron, which is responsible for developing information warfare tactics, and before that he was chief of defensive information warfare integration, Directorate of Intelligence, Surveillance, and Reconnaissance, Headquarters USAF. He has also been an assistant professor of political science at the Air Force Academy and deputy director of the USAF Institute for National Security Studies. From 1989 to 1991 he served as an intelligence officer at Headquarters Strategic Air Command, dealing with arms control and national intelligence estimates, and from 1987 to 1988 he was with the 18th Tactical Fighter Wing, Kadena Air Base, Okinawa, Japan. He is the author of Strategic Warfare in Cyberspace *(MIT Press, 2001). He has a bachelor's degree in international affairs and military history from the Air Force Academy, a master's degree in public policy from the John F. Kennedy School of Government, Harvard University, and a doctorate in international security from the Fletcher School of Law and Diplomacy, Tufts University.*

Oettinger: Some of you have had the occasion to meet today's first speaker, Colonel Rattray. All of you should by last week have read his book. It's a particular pleasure to introduce him because he is an alumnus of this seminar, now in high office, and I'm glad to welcome him back. It's all yours, Greg.

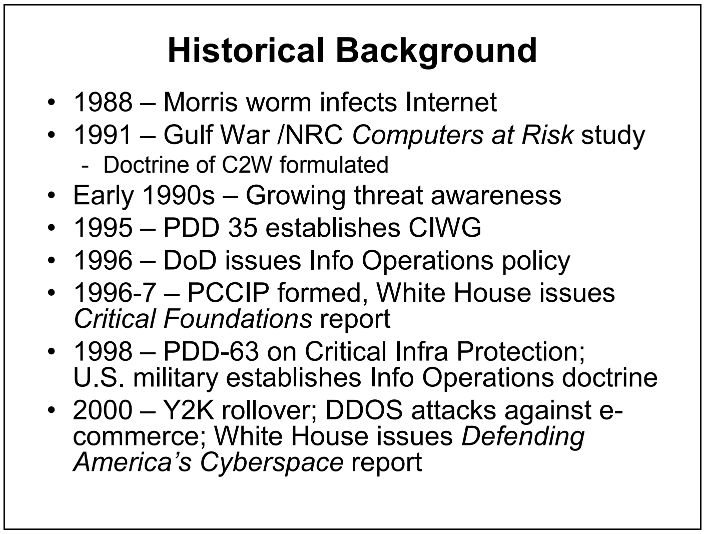
Rattray: Thank you. It's enjoyable for me to be back at a lot of levels. I grew up in Wakefield, Massachusetts. Some of you may know where that is: it's about ten miles north of here. I came back to the MPP [master's of public policy] program here at the Kennedy School in 1984, which doesn't seem that long ago to me, but probably seems like a long time to some of you. Finally, I got the opportunity to come back again in the mid-1990s and work with Tony. It was then that I really got into this area: information warfare, cyber security, and cyber warfare.

What I want to explain to you is what cyber security looks like from the perspective of the White House. I'm going to talk a little about how this concern has developed over time. If you did actually wade through the book you'll realize that this is kind of fundamental to my perspective: organizations, studies, blue-ribbon panels, and bureaucratic change are important. Basically, you can have the best ideas and concepts in the world, but more important is the way we operationalize as we set up organizations to apply resources (or not) and to create capacity to undertake activities such as secure cyberspace. So, while it’s not the most exciting material given that you are students of public policy trying understanding what the United States can do to protect the nation’s cyberspace, I’m going to lead you through some of that bureaucratic history.

I will also discuss a document titled the *National Strategy to Secure Cyberspace*.[1] I would encourage you to read it. This is the president’s declared strategy about what we’re trying to accomplish in this area. I will tell you that the Department of Homeland Security [DHS] uses this strategy to guide their efforts. I’ll provide my perspective on what it says. That will probably take about an hour of what I hope will be an interactive discussion. From what I saw at lunch, I expect a lot of questions as I go through.

In the second portion of our time, I will switch to a more conceptual discussion about what strategic warfare would look like in cyberspace. If you did your homework, read the book, and wrote your one-page paper (if that’s still the modus operandi for the seminar) you’ll have all the answers for the things I want to discuss in the last forty-five minutes of the session.

I’m not going to go through all this (**Figure 1**). When I personally started looking at this it was 1995 and most people said, “This is a brand new problem.” When I sit here in 2004, it seems we have been working this problem for some considerable period of time. 1988 is an artificial starting point to describe an evolution of events. A lot of conceptual and policy formulation has



Historical Background

- 1988 – Morris worm infects Internet
- 1991 – Gulf War /NRC *Computers at Risk* study
  - Doctrine of C2W formulated
- Early 1990s – Growing threat awareness
- 1995 – PDD 35 establishes CIWG
- 1996 – DoD issues Info Operations policy
- 1996-7 – PCCIP formed, White House issues *Critical Foundations* report
- 1998 – PDD-63 on Critical Infra Protection; U.S. military establishes Info Operations doctrine
- 2000 – Y2K rollover; DDOS attacks against e-commerce; White House issues *Defending America’s Cyberspace* report

C2W = command and control warfare CIWG = Critical Infrastructures Working Group DDOS = distributed denial of service NRC = National Research Council PCCIP = President’s Council on Critical Infrastructure Protection PDD = Presidential Decision Directive Y2K = Year 2000

Figure 1

[1] *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, February 2003), [On-line]. URL: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (Last accessed on 27 December 2004.)

occurred over what I'm characterizing as a fifteen-year timeframe. I want to highlight that there are two threads weaving together in that timeline: an understanding that the civil sector relies on computers and that those computers can be disrupted, starting with the Morris worm in 1988.

Oettinger: I just wanted to point that Robert Morris was an undergraduate in computer science here at Harvard, but he wrote the worm while he was a graduate student at Cornell.

Rattray: So the root of the problems is here, but they sprout when everybody leaves!

Oettinger: His father also was a computer security expert at the National Security Agency. The whole thing was a great embarrassment.

Rattray: But it did result in problem recognition at a national level. If you want to look at an early document in this field and judge how much progress we've made, read that 1991 National Research Council report called *Computers at Risk*.[2] The challenges I'm going to talk about were basically all pointed out in 1991.[3] In some ways that's good, because it's a result of our not having

suffered a sufficiently catastrophic event or series of events that radically changed the dynamics of the field. However, I think our approach to this field is ossifying in a way that's not particularly good.

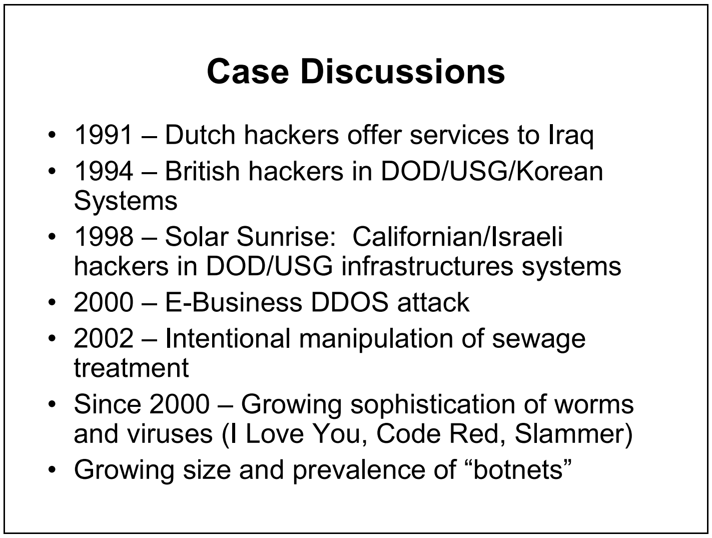
The other thread that runs through this is the military aspect. A growing recognition began with the Gulf War that our military operations are dependent on information systems and therefore we have to secure these systems so that we can dominate the battlespace as well as use the information domain as a way to shape our adversaries' perceptions. I've been very much involved with these efforts over the course of the last ten years, and the government and private sector communities have played off each other in terms of increasing energy devoted to these issues.

I don't really want to go through a long discussion of each of these incidents (**Figure 2**). We had a discussion at lunch about what precipitates public attention. For cyber security, attention has stemmed from hacker incidents and press reports. Actually, some of these incidents were sensitive when they occurred, such as the 1994 hackers from the United Kingdom who compromised DOD [Department of Defense], other U.S. government, and Korean computers, but then they became publicly recognized, often through General Accounting Office reports. Some of these events engaged the senior leadership of the nation and motivated the type of policy developments that you saw on the previous slide.

To my mind, these events indicate an increasing scale of effect. There was the incident in the spring of 2000 when a number of businesses that transacted commerce on the Internet got

[2] National Research Council, Computer Science and Telecommunications Board, *Computers at Risk*: *Safe Computing in the Information Age* (Washington, D.C.: National Academies Press, 1991), [On-line]. URL: http://www.nap.edu/books/0309043883/html/index.html (Last accessed on 27 December 2004.)

[3] The full set of slides prepared for this presentation is available on the PIRP Web site at URL: http://www.pirp.harvard.edu/courses/ISP483_Spring2004/RattrayCybersecurity%20-%20Spring%2004.ppt



Case Discussions

- 1991 – Dutch hackers offer services to Iraq
- 1994 – British hackers in DOD/USG/Korean Systems
- 1998 – Solar Sunrise: Californian/Israeli hackers in DOD/USG infrastructures systems
- 2000 – E-Business DDOS attack
- 2002 – Intentional manipulation of sewage treatment
- Since 2000 – Growing sophistication of worms and viruses (I Love You, Code Red, Slammer)
- Growing size and prevalence of “botnets”

USG = U.S. government

Figure 2

attacked by someone who turned out to be a kid in Montreal. Their ability to conduct e-commerce was disrupted, usually only for a period of hours, but it resulted in President Clinton’s holding a national summit and calling in all the cyber security experts. This incident began to cross the threshold of national significance. We have yet to suffer an orchestrated cyber attack by anybody except an individual, in terms of a disruptive event of national security significance. But we do see evidence of increasing capacity if one were trying to orchestrate that activity to cause disruption.

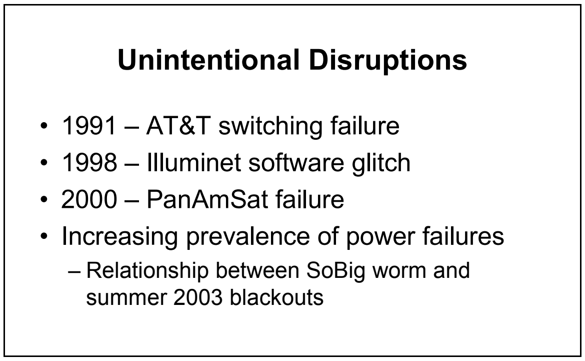
I put in the intentional manipulation of a sewage treatment system in Australia. This incident resulted from access that a disgruntled employee had to the computer control system. He used the knowledge he had about how the SCADA [supervisory control and data acquisition] systems worked to release sewage into the water supply for the city and therefore the water was undrinkable for a period of days. I highlight this event because it illuminates a fundamental concern: that our infrastructures increasingly utilize digital controls and there is the potential for adversaries to use these control systems for malicious purposes. Dams, water systems, manufacturing systems, and transportation systems, to the extent to which they rely on automated controls, become potential targets of disruptive attacks. Technically, the possibility is there. Under what conditions the potential threat could become real mostly remains to be seen.

You are probably familiar with the increasing frequency of worms that move very quickly throughout computer networks. My basic take on this phenomenon is that the system is adapting well to this sort of eventuality. The Internet service provider community—the organizations and people who provide your Internet connection and keep the bytes flowing—now have had enough experience that they’re identifying and mitigating the adverse effects of worms more quickly and understand their impacts, although some interesting problems always continue to crop up. The ATM [automated teller machine] problems within the Bank of America during the Slammer worm occurred on a system that supposedly was not connected to the Internet. In the financial sector, some argue that their systems are protected because they are largely on dedicated circuits that don't intersect with the Internet. However, the complexity of these infrastructures is such that no one who uses them really understands how and when interconnections may occur. That's an uncertainty that we're trying to deal with more effectively.

Do you understand what I mean by botnets? They are becoming increasingly worrisome as a cyber threat. A bot is a piece of software that allows remote access and some degree of control over the computer it resides upon from a remote computer. We now have large networks of computers that basically have such code embedded in them. Your home computer, particularly if it has a broadband connection that is always on, could easily be the target of a virus or a worm. That worm will embed itself in your system and turn your computer into what we call a zombie. The real danger of these worms is not what gets disrupted day to day. It has to do with the control over large numbers of computers attained by the people who run these botnets. They could be malicious actors. Often they are kids trying to see how many computers they can control; they claim on Internet chat rooms that they number in the tens of thousands. However, these botnets can be run by organized crime trying to get control of credit card numbers or to produce spam for profit.

One thing that I think is not well recognized is that we have an increasingly dire situation in cyberspace where sets of computers, unknown to the owners of those computers, are under the control of third parties. This poses an interesting set of national security, law enforcement, and other concerns in terms of who has the right to notify whom to do what to remove these botnets. Their scale is particularly troublesome when they start to number in the tens of thousands of computers that aren't located in any specific organization. They result from the successful spread of worms that have diffused through and across geographic borders, certainly across public and private sectors. As you can see from these examples, a lot of different types of activities occur in cyberspace that may or may not be of national security significance.

None of those events that I talked about, which were the result of somebody maliciously trying to do things, had the same level of impact as unintentional events stemming from human error, such as coding errors resulting in bad software that was loaded into basic telecommunication switches (**Figure 3**). In another case, the dissemination of a glitch in a little-known signaling system produced by a small company called Illuminet caused outages of television stations and other telecommunications-reliant companies. The AT&T switching failure mentioned on the slide lasted for the greater part of a day and affected approximately 70 percent of AT&T calls, which in



Unintentional Disruptions

- 1991 – AT&T switching failure
- 1998 – Illuminet software glitch
- 2000 – PanAmSat failure
- Increasing prevalence of power failures
  - Relationship between SoBig worm and summer 2003 blackouts

Figure 3

1991 was a significant portion of the market, though it is much less significant now than it was then. The PanAmSat outage may have been caused by natural phenomena in space. The PanAmSat communications satellite went out; therefore, most people's pagers didn't work, because SkyTel used that satellite to provide paging services. There were other services depending on that satellite.

Bob Liscouski, who will talk to you later this afternoon, mentioned at lunch the intersection of the SoBig worm and the blackouts in the summer of 2003. The worm affected control systems used by people who were trying to remediate what was going on with the power outage and actually blinded them to aspects of what was happening. While we do not assess this event as having been an orchestrated attack, it shows again the potential for cyber disruption at the same time as other problems to cause cascading failures.

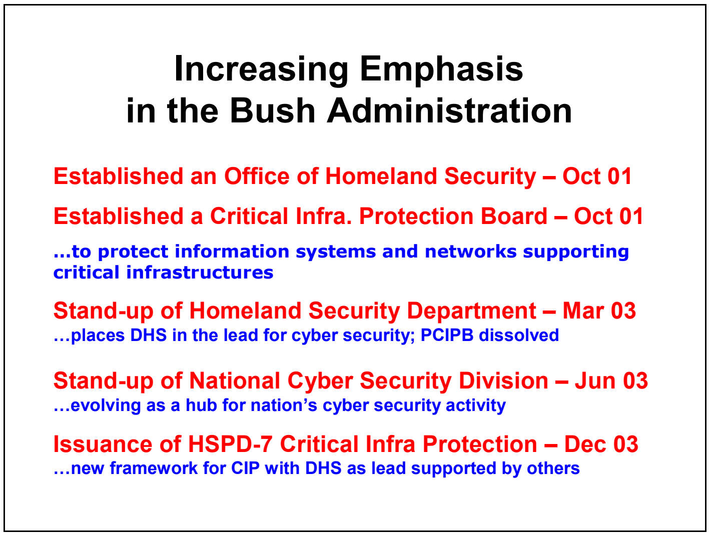
I'm going to say in the same breath that the systems that failed generally recovered quickly with the exception of the last one, which was a very prolonged blackout. The disruptions usually only lasted for hours. So the system also has a degree of resilience. It may have a very high degree of resilience.

Something I should have put on the slide but didn't was Y2K. We invested some billions of dollars in Y2K as a potentially horrendous situation. It's in the epilogue of the book. One of the things that Y2K taught us was that while there were problems related to the switching over of the date function within software the disruptions were really limited. So there is a lot of inherent flexibility, robustness, and adaptability in the systems and the people who use them. To my mind, we do not know yet how this plays out in most large-scale scenarios of national security concern.

Oettinger: I just want to comment that there is a glass-half-full and a glass-half-empty aspect to this. If you look at the disruptions that followed 9/11, you can view them as a disaster for the financial services community and so on. You can also view them as a triumph of rapid restoration. How you evaluate that depends on the mood of the day.

Rattray: I won't bore you with all the administrative aspects of this, but the Bush administration was planning to form a critical infrastructure board and, to my knowledge, was actually going to announce the standup of the Critical Infrastructure Protection Board on September 11 (**Figure 4**). That was delayed a month and became part of the nation's focus on homeland security. I arrived at my current job in the summer of 2002 and watched us move from a White House-centric management of homeland security to the standup of the DHS. You have a unique opportunity to have Bob Liscouski here. Talk to him about the challenge of combining numerous government organizations with different missions and concerns and putting them together to do things such as protect critical infrastructure.

My piece of what Bob does involves the National Cyber Security Division [NCSD] in the DHS. The creation of NCSD is significant. The president's direction put the DHS squarely in the lead for critical infrastructure protection, supported by the other government agencies. That



Increasing Emphasis
in the Bush Administration

Established an Office of Homeland Security – Oct 01

Established a Critical Infra. Protection Board – Oct 01

...to protect information systems and networks supporting critical infrastructures

Stand-up of Homeland Security Department – Mar 03
...places DHS in the lead for cyber security; PCIPB dissolved

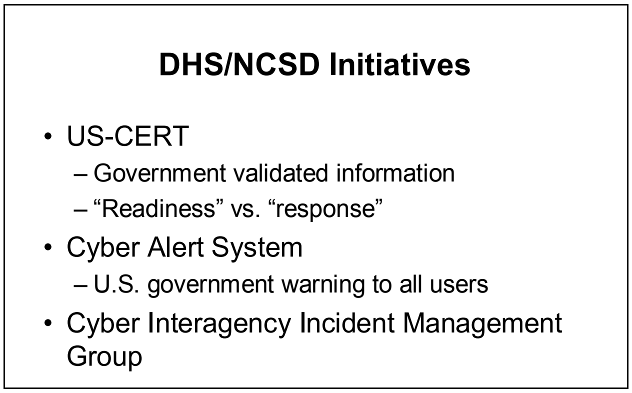
Stand-up of National Cyber Security Division – Jun 03
...evolving as a hub for nation's cyber security activity

Issuance of HSPD-7 Critical Infra Protection – Dec 03
...new framework for CIP with DHS as lead supported by others

Figure 4

direction was detailed in something called HSPD [Homeland Security Policy Directive] 7.[4] For policy wonks, we have a system of NSC directives called NSPDs, National Security Policy Directives. The Homeland Security Council [HSC] was established when the DHS was stood up and so it's a parallel structure to handle interagency homeland security issues. That council issues HSPDs.

The next slide describes how NCSD is trying to organize efforts within the government and reach outside the government to provide operational capability (**Figure 5**). Unless you spend some time working in large organizations and have the opportunity both to work out in the field



DHS/NCSD Initiatives

- US-CERT
  - Government validated information
  - "Readiness" vs. "response"
- Cyber Alert System
  - U.S. government warning to all users
- Cyber Interagency Incident Management Group

Figure 5

[4] Homeland Security Presidential Directive/HSPD-7—Subject: Critical Infrastructure Identification, Prioritization, and Protection (Washington, D.C.: The White House, December 17, 2003), [On-line]. URL: http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html (Last accessed on 27 December 2004.)

and to serve on headquarters staffs, you may not realize the fundamental limitations that headquarters staffs can have. Initially during my tenure at the White House, I was on the President's Critical Infrastructure Protection Board. We had sixteen staff members and were trying to operationalize the nation's capacity to do cyber security: set policy and stand up in public forums and say what the right answer was. That's a much more limited mechanism than empowering a department with real budgetary and personnel resources to formulate organizations such as the NCSD. There has been a lot of criticism of the administration's approach to cyber security. I don't think most critics realize that having a department with an operational mission and mandate to work with the rest of the federal government and the private sector to do cyber security is a really big step forward.

Oettinger: But as you'll hear from Bob Liscouski, it still is a very small step compared to the magnitude of the task, which isn't going to get done unless the private sector does it. There is never going to be enough tax money or knowledge for government bureaucrats to do it all. Whether you aim at public or private careers, an important issue to keep in mind is that the buck stops with all of us.

Rattray: I completely concur with Tony, and so will Bob. My reference to a big step forward is that even within government our ability to work with the private sector so they can secure their own systems and to organize ourselves is much greater now that it's been pushed to an operational organization that is responsible to the president. When I was a student, I remember a tendency to focus on what happens at the highest levels of the system as opposed to the organizational capacity that's being built out within government and, in the case of cyberspace security, also where government has to work with the private sector.

NCSD is doing a number of things. It has created for the first time a U.S. government CERT [computer emergency response team]. We've long had a largely government-funded CERT at Carnegie Mellon University. It was a very effective mechanism to give advice to people who had information security problems. They would come to this nonprofit organization. Increasingly at Carnegie Mellon they provided information about how to solve these problems. Private sector organizations have been created in the last five years or so that also provide advice, particularly to corporations, about what vulnerabilities systems have and how to patch vulnerabilities in computer and other technical systems.

Amit Yoran currently runs the NCSD.[5] Amit's vision is that he wanted to have an official U.S. government system not driven by a profit motive where corporations and individuals could get U.S. government-recommended steps about how to mitigate significant cyber security problems. That's what I mean by "government-validated" information on the slide. The other thing that Amit did was change what "CERT" meant, at least for his CERT. His CERT is about readiness as well as computer emergency response. The NCSD organization is as much about telling people how to prevent things from happening—readiness, as it is about reacting to things—response. He has also instituted what's called a cyber alert system, which pushes out warnings through the CERT in a structured fashion both to nontechnical communities, such as

[5] Amit Yoran resigned in October 2004. US-CERT is currently led by Donald A. (Andy) Purdy, Jr., the acting director of NCSD.

home users, and to the more technical system administrators in large enterprises. He pushes out more sensitive information to a more trusted set of players, but anybody can go to the US-CERT Web site and see what cyber alerts are out there.[6] Within the first two weeks they got more than 500,000 subscribers to their cyber alert warning system.

Oettinger: If it were earlier in the semester, there is a term paper topic lurking there, because there is an outfit called the SANS Institute [SysAdmin, Audit, Network, Security], which is a private sector initiative that does essentially what you have described. It has been in operation for a while, initiated by systems administrators across the board. Would you say what differentiates the US-CERT from what SANS does?

Rattray: SANS is largely an educational organization and as a result its focus is on educating system administrators about how to secure their systems. The organization also puts out information, such as a recent study about the value added of different ways of sharing information security information. I think the US-CERT's take on its value is that the resources of the U.S. government have been added to the mix in terms of analyzing the significance of the information, so you get better prioritized (at least from the government's perspective of what's important) information about what you should do.

Providing information on cyber attacks and warnings of worms or hacker activity is an area where there are a lot of organizations vying for attention, some of which have a profit motive. For instance, there are Symantec, the antivirus company, and an organization called I-Defense, which is basically in the business of discovering vulnerabilities and warning people. There are others with the public interest at heart. We hope that's what the government has.

Another facet is that US-CERT is particularly attentive to the balance between timeliness and accuracy. There are a lot of situations where you get reporting that something is coming up or emerging. Intelligence is fraught with this debate. When a worm comes out or a vulnerability is discovered in Microsoft's software, there is conflicting information about its significance, how it works technically, and how to remediate it. If you don't get that information out soon enough, people can take advantage of that vulnerability. If you let it out too soon, you're facing a potential problem in having to go back and correct yourself. People may have taken inappropriate actions in the interim and might criticize the early warning as a mistake. The government owes the public its best effort at striking that balance. Organizations such as SANS tend to wait longer in issuing warnings than the US-CERT does.

The Cyber Interagency Incident Management Group is a long title for something that is at the core of my concern. This group will be the mechanism for how the DHS pulls all the U.S. government agencies together and decides what we ought to do in the case of different incidents. That's worth a long discussion. If something happens in cyberspace and we need awareness, particularly concerning the significance of a vulnerability and ongoing malicious activity, this group orchestrates how we're all going to try to get on the same sheet of music about what the U.S. government will do about it.

[6] The URL is http://www.us-cert.gov

Oettinger: Just to reiterate something you said earlier, this sounds like bureaucratic Mickey Mouse. But think about it: it has a lot to do not only with bureaucratic turf but also with who picks up the ball. If there is no understanding it might be nobody or, at the other extreme, there might be folks scrambling over one another.

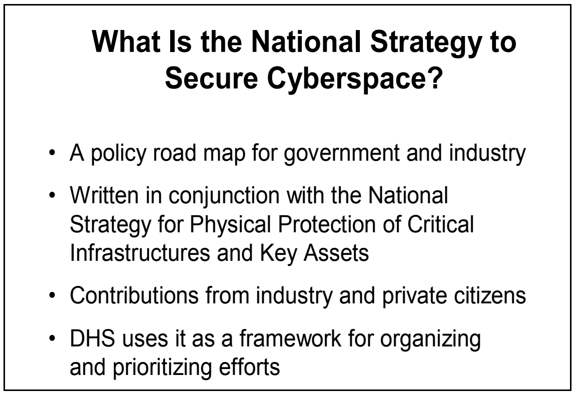
I don't know how many of you watched the television news this morning about a little girl who spent five days in the open after her mother died in a car crash. They were interviewing the police chief of Indio, California, and he acted helpless. He said, "This happened outside our jurisdiction." He said they spent the whole morning looking in the Indio area, and it wasn't until much later that they alerted some of the folks outside. So, it's a question of who has jurisdiction and who is responsible. It gets hairy as heck here. If the "incident" is somebody looking at your files, it might be either the FBI [Federal Bureau of Investigation] investigating you for possible theft or somebody interested in counterintelligence prying into your files just because it's the French or the Indians or somebody. So there is a lot at stake here, because it's a large world. You can't have it monolithic, so you divide the responsibility. The minute you divide the responsibility the question arises who in a particular situation is responsible for what. It's a messy problem.

Rattray: A later slide talks about all the other government agencies besides the DHS that have important roles. That group that we just discussed, the Cyber Interagency Incident Management Group (we need to get a nice, spiffy bumper sticker for that), would be the place where, if a worm is infecting the financial sector and starts to demonstrate malicious characteristics, Department of Justice and FBI will talk about what they're doing on a law enforcement basis to find the person who authored that worm. We discuss whether the activity looks like an operation to create back doors for an adversary intelligence organization, which creates a counterintelligence challenge. Is it disrupting the infrastructure, which is DHS's responsibility? There is no natural locus and no single responsibility to respond in these situations.

Moving from bureaucracy to the conceptual framework for what the bureaucracies should be doing, which is one way of describing what a strategy is, we do have a presidentially signed strategy: the *National Strategy to Secure Cyberspace*. It is not focused solely on government (**Figure 6**).

We issued the strategy in conjunction with the strategy for physical protection of critical infrastructures. I think you will hear Bob [Liscouski] talk about how cyber is not an activity unto itself, and I will talk about it a little bit later. There are physical vulnerabilities to our cyber infrastructure. There are actions an adversary can take in cyberspace that can amplify the effect of a physical attack. The government now is trying to work these things as conjoint problem sets. We will talk about the industry and private citizen aspect.

Oettinger: Before you go on, there is a kind of mind-boggling dualism here. Just when the distinction between mind and body is being removed by modern and biological science that generally locates the mind in the body, we are perpetuating this nonsense by distinguishing cyber as kind of a mind distinct from a physical kind of body. I emphasize this because Greg in his book (and a couple of you did notice it) rectified this error by pointing out that anything that happens in



What Is the National Strategy to Secure Cyberspace?

- A policy road map for government and industry
- Written in conjunction with the National Strategy for Physical Protection of Critical Infrastructures and Key Assets
- Contributions from industry and private citizens
- DHS uses it as a framework for organizing and prioritizing efforts

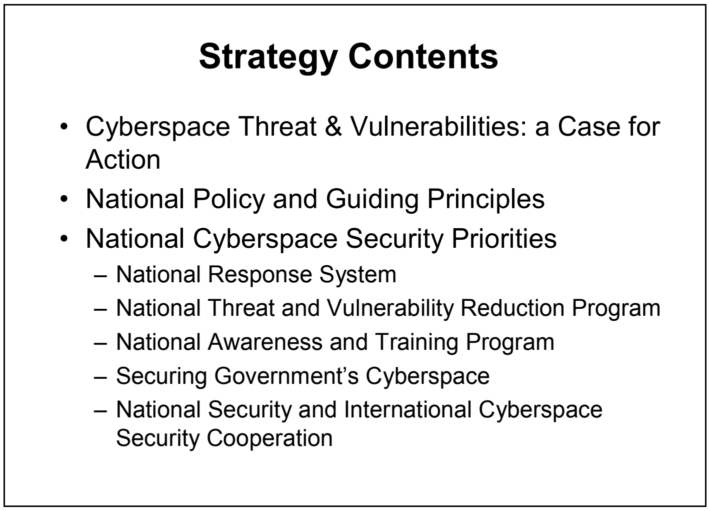
Figure 6

cyberspace is not disembodied. It's just that the amount of energy involved in screwing around with things or doing things in cyberspace is very small compared to, let's say, an ordinary bomb or the energy necessary to fire a bullet. He coined the term "microforce" that he used to describe cyberspace. The reason for emphasizing this is that there is nothing so terribly mysterious about cyberspace. It's just like anyplace else, except that the amount of energy involved in doing things is relatively small. It's not disembodied any more than in modern usage the mind is disembodied. Does that make sense?

Rattray: Yes, and I'll tell you that this concept is probably fairly well understood in the cyberspace security community. When I got into this almost ten years ago, there were a lot of statements to the effect that "Cyberspace is a realm of the noncorporeal and operates independently of what happens in the physical world." Now, in terms of our strategies to protect the United States and its critical infrastructure, we have very much recognized that a telecommunications hotel hosts routers that have magnetic memory and wires that carry electromagnetic signals, and there a lot of ways to disrupt that magnetic memory and those signals. You can blow them up or you can hack into the memory and change the orientation of the magnetic things that represent ones and zeros. I actually think we've gone a good way in that regard.

This strategy is significant, because now that an organization in the U.S. government is responsible for protecting cyberspace, this is the national strategy that guides DHS's approach. I'm going to walk through the bottom five sub-bullets, so I won't get into them here (**Figure 7**).

I talked to you about threats. I didn't talk a lot, but I will if you want, about vulnerabilities. Vulnerability boils down to the fact that as you become more reliant on "information systems," broadly defined, that are controlled digitally, thereby being in cyberspace, the disruption of your ability to use those systems poses a vulnerability to getting things done: command military forces, have electronic banking transactions, and so on. We are increasingly reliant on these information infrastructures, and their technological foundations are increasingly more difficult to secure, though maybe not inherently less robust. Their complexity and the increasing dimensions of access to networks, such as through wireless devices, present a lot of potential vulnerability. It's the significance of those vulnerabilities that's hard to analyze.

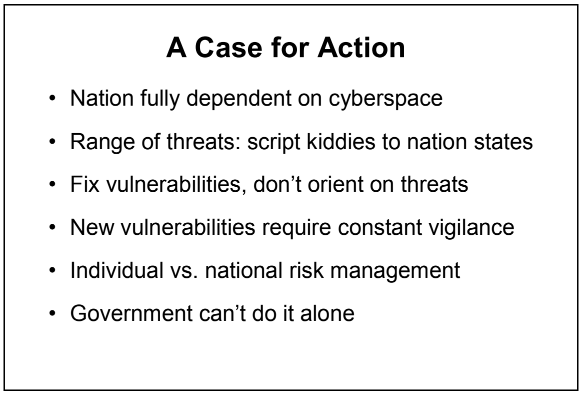


Strategy Contents

- Cyberspace Threat & Vulnerabilities: a Case for Action
- National Policy and Guiding Principles
- National Cyberspace Security Priorities
  - – National Response System
  - – National Threat and Vulnerability Reduction Program
  - – National Awareness and Training Program
  - – Securing Government's Cyberspace
  - – National Security and International Cyberspace Security Cooperation

Figure 7

I'll let you read through the bullets in this next slide (**Figure 8**). I ask you to challenge me on any of the bullets and explain why we put them in the strategy, and discuss whether you think things are not on these slides that should be. We could have a long discussion about what types of actors pose what threats to the vulnerability that results from our relying on cyberspace to function properly.



A Case for Action

- Nation fully dependent on cyberspace
- Range of threats: script kiddies to nation states
- Fix vulnerabilities, don't orient on threats
- New vulnerabilities require constant vigilance
- Individual vs. national risk management
- Government can't do it alone

Figure 8

I do think we need to limit the number of vulnerabilities in cyberspace, but as an intelligence officer (getting back to how your background affects how you perceive problems) I tend to focus on understanding which actors in the system want to do something bad to something that is of concern to me. The United States or an infrastructure can have all the vulnerability in the world yet be comfortable if there is no one out there who wants to do anything malicious. Who is threatening you, what their capacity is to do harm, and what they want to achieve if they do harm to you is important if you're going to take a risk management approach and therefore fix the vulnerabilities posed by the adversary that presents the most threat to you. I think both sides of the vulnerability–threat equation are important.

Oettinger: Let me just put in a plug for Dan Knauf, a previous Air Force Research Fellow of the Program (he was actually an NSA [National Security Agency] researcher), who wrote a paper on this very issue in which he introduced a third term of "susceptibility" to help make the point that Greg just made.[7] You don't worry about a vulnerability for which there is no threat, but susceptibility implies that not only are you vulnerable to something but there is also a threat. You're susceptible to catching cold, for example. We're all vulnerable to colds, but if we wash our hands and don't expose ourselves, et cetera, or if we're in a sterile environment, we won't necessarily be susceptible. So this notion of susceptibility, combining the ideas of threat and vulnerability, is another way of expressing what Greg just said.

Rattray: I used a diagram of his in the book to illustrate this point.

Student: It doesn't really make much sense in terms of how we're trying to work with counterterrorism. Maybe up until September 11 we had that viewpoint on homeland security. Is it going to take an attack like September 11 and somebody who really causes some type of catastrophic cyber terrorism event for us to identify who's causing threats? How do you know what the vulnerabilities are unless you do that red–blue teaming as intelligence officers do?

Rattray: I think there are two different things going on here. First, red-teaming yourself to understand your vulnerabilities is important. There is a lot of that going on; there should be more of it. The dominant paradigm, focused on closing all vulnerabilities, is counterproductive in the cyber security field. It stems from the fact that in cyberspace it is really hard to figure out who is threatening out there. Access to intrusive or disruptive capabilities is fairly broad, so the intelligence challenges of defining the threat capabilities are really tough. In light of that—and I think this is abrogating the responsibility to do good analysis and prioritize your efforts—the basic approach is "Let's just fix it all." If we fix as much as we can of the vulnerability, the significance of all the threats (recognizing they are out there) is suppressed. My concern is that sophisticated actors are going to find access points into our networks no matter how hard we work on patching vulnerabilities. All they need are a few vulnerabilities present in the hard outer shell of most networks and basically they're really going to wreak havoc once they've established access inside.

Student: We tend to be reactive versus proactive. If you look at airlines, it's as though maybe we thought we were secure with the airlines because we secured luggage, and then somebody used a shoe bomb.

Oettinger: Do you have steel shutters on all the windows in your house?

Student: No, I don't.

[7] Daniel J. Knauf, *The Family Jewels: Corporate Policy on the Protection of Information Resources* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-91-5, June 1991), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=85

Oettinger: Well, there you are. If I came by with a bazooka and blasted through your window, you could be sleeping quietly in your bed and you'd be dead. You don't practice what I hear you preaching.

Student: No, but I think there is a difference between what's an acceptable loss on some individual level versus the national level. I don't secure my home because the cost is too high.

Oettinger: Think about the cost to the government for securing cyberspace! It's our money.

Student: I recognize that. I just think that the mindsets are different. How would you know about the vulnerability unless you try to understand the threats?

Rattray: We do red-team, and that is one of the ways we try to find the vulnerabilities.

Student: That is where I'm trying to draw this distinction. Maybe you don't orient on a specific person, but you somehow then get into the mindset of somebody who might do something, just as we may not know who individual terrorists are but we should get into their mindset.

Rattray: We could characterize terrorist groups capable of cyber attacks as a generic phenomenon, and then put a red team out there to act like our generic terrorist and see what they could potentially do. Then we need to make sure we're fixing the vulnerabilities we think that group is capable of attacking.

Student: I guess my point is that you're getting in a red-team mindset anyway to say how we might be vulnerable. If you determine that somebody could come in through a particular way you're still focusing on the threat.

Rattray: They can find a lot of vulnerabilities and we're going to have to prioritize our vulnerabilities in remediation efforts. That, to my mind, has to depend on which threats you think are particularly severe. Basically, to figure out which vulnerabilities to fix you have to have an idea about which threats are most dangerous. That is the step that, as far as I'm concerned, is unattended to.

Student: The security lexicon is not terribly good when it comes to threats. The term "threat" can be used to mean the threat scenario—something somebody does, or a threat source—that is, the person who will be attacking you, the adversary, the actor. Which way are you using it as here?

Rattray: To me, "threat" has two, or maybe three, dimensions. First, it's an intent to do harm. The Brits, arguably, may have a lot of capacity to do harm, but we don't conceive of them as a threat. There are plenty of unsophisticated non-state actors that have absolutely no technological savvy, so while they may want to wreak havoc in cyberspace they have no capacity to do so either technologically or in terms of targeting what they might want to break.

Oettinger: On the other hand, if you compare the college degrees and knowledge of some of Al Qaeda's leadership with those in this country they'd come out pretty well.

Rattray: They would not be the group I would characterize as technologically unsophisticated. The question there is if any group of concern is employing its capacity to do the background analysis that's necessary to do harm in cyberspace. The two big things I focus on are: do the actors intend to do something, and do they have the capacity to do something?

Student: It sounds as though you're using "threat" as the source individuals, because you can't really ignore the actor. When you use "threat" to mean the threat scenario, a vulnerability has to be defined in terms of a scenario. For computer security there are vulnerabilities that allow confidentiality to be compromised, so your scenario there is that someone is going to get information out of your system and use it somehow. But that's not a vulnerability: you're an open system and your purpose is that anyone should be able to read anything.

Rattray: The intent drives the scenario. Let's say there is a country that we don't think would disrupt us, but would want to seek military/industrial information from us. That poses different threat scenarios based on intent. Cyber espionage is threatening to national security, and there are actors who are capable of it and intend to do it that might not pose a disruptive threat.

Student: What I'm saying is that if you're focusing on vulnerabilities, you have to ask "How much do I care about this vulnerability?" You could spend all your resources going after one type of vulnerability, and if you haven't thought about which threat scenarios you actually care about this could be an impossible situation.

Rattray: Agreed. Maybe this thought would help, too. As a national concern, credit card number theft at some aggregate level would be a threat when it undermines the ability of the financial industry to issue credit cards and have people be confident about their transactions. But generally the fact that individuals can steal credit card numbers from computers doesn't rise to the level of a national security threat. Therefore, while I hope banks are doing what is in their own interest to protect themselves against credit card number theft and that businesses that process credit card information are protecting themselves, the government's effort, the national security effort, is not going to be aimed at protecting against that specific threat. The Treasury Department and FBI may be expending effort on helping businesses secure their infrastructure, but I think that's the point you're getting at.

Again, you have to have an idea of what sorts of scenarios, what sorts of malicious intent, as well as what sorts of capabilities you need to defend against. This gets back to my intelligence background. I think of a strategy generally as a dimension of "You've got to understand your adversary and its objectives to order to prioritize your efforts." You allocate limited resources to protect and react based on what you project the adversary might do. This is a very conceptual debate, but it's very fundamental. What I hear when I go to a lot of cyber security meetings is: "Let's just put the shields up and build the castle walls as high as we can. How high should they be? I don't know, but they're not high enough yet, so just build them higher." To me that doesn't provide a basis for a rational investment strategy.

Oettinger: You may want to pursue that point further with Bob Liscouski, because he lives with this. Part of his job is to figure out how high those walls should be built for the government, and you'd be surprised at some of the answers you get from him.

Student: Maybe you're going to address this later, but, despite what the third bullet says, as an intelligence officer who does think about the threats would you care to name what you think are the top three threats?

Rattray: I'm concerned about major strategic competitors of the United States being able to use cyberspace asymmetrically against us. In other words, if we were to get into a war with somebody, they could actually disrupt both our military operations and other things of concern to the nation as a way of fighting back against our military forces.

I'm concerned about cyber espionage: that people who want to compete with the United States economically and/or militarily can in peacetime competition get access to our secrets. We don't give an advantage to our firms by conducting economic espionage. Other countries do. We do try to help our firms protect their sensitive information.

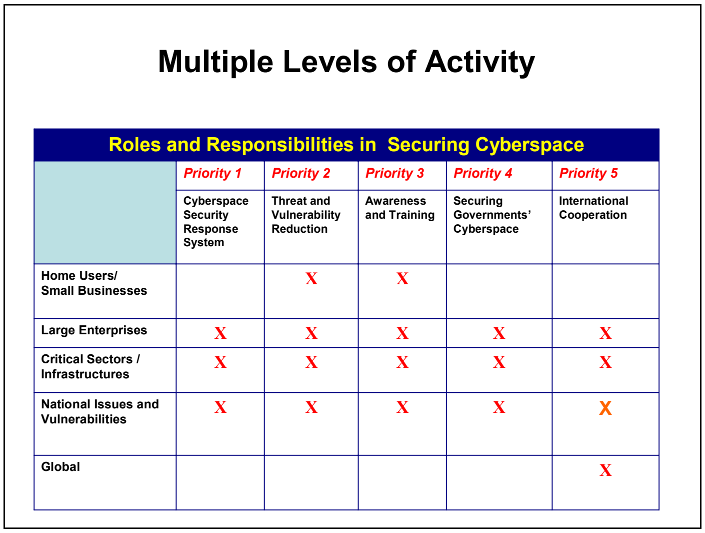
The other major concern I have is with situations like the one we faced as war loomed with Iraq. (We're off on a tangent, but I think it's a useful one.) When we were going into the war in Iraq, my concern as a cyber security guy was what the Iraqis could do to us in cyberspace. Time proved they couldn't do much. We also had to consider whether there were capacities to undertake cyber attacks in the Islamic world—even if not necessarily orchestrated by the Iraqi government—that could be motivated to take action in this area. Also, we thought about whether an antiwar movement might arise in the United States where for the first time disruption of government systems in cyberspace could become a part of the protest movement. Fortunately, those things did not occur. Are we ready for these types of contingencies? We've got to be able to react to the unexpected. So I guess those are my three macro-level threat concerns.

Student: Just a quick follow-up. If 10,000 Chinese guys email decision makers in government with a bunch of harangues because we changed a policy, in your view is that a cyberspace attack or is that just propaganda and not within your purview?

Rattray: This scenario involves an interesting intersection between perception management—the use of a variety of media to influence other countries' leadership and populations (and cyberspace is one of those media)—and cyber security. Currently it's a shared responsibility throughout government to deal with such situations.

I'm going to continue to step through these slides (**Figure 9**). This information is all in the national strategy. This matrix illustrates the need to attend to cyber security not only as a government concern. My particular job responsibilities focus more on the last two levels, though intersecting with that third level. The HSC really covers the top three levels intersecting with the fourth.

We started to talk about this already (**Figure 10**). Read through the bullets. While we must fix vulnerabilities, my opinion is that we're never going to fix them all. A sophisticated threat will always be able to cause problems, so we ought to be investing some resources in how we respond to the problems once we detect them. My concern is that our investment structure is 90 percent focused on prevention and only 10 percent focused on response. What is the right balance? One

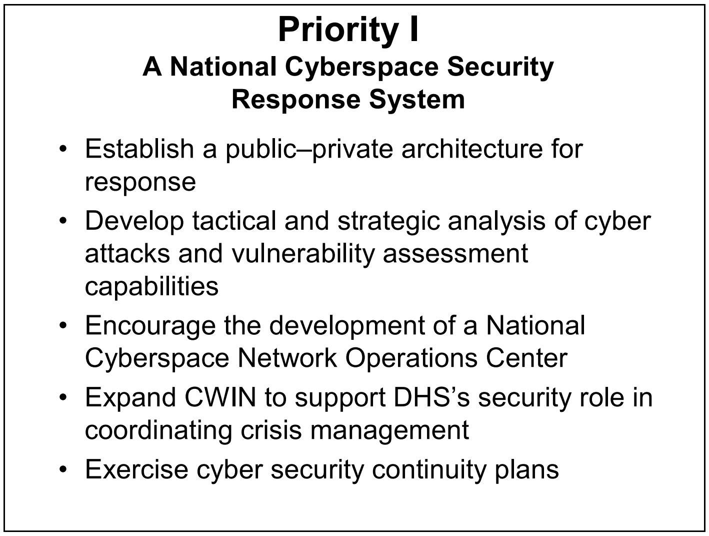


Multiple Levels of Activity

Roles and Responsibilities in Securing Cyberspace

	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5
	Cyberspace Security Response System	Threat and Vulnerability Reduction	Awareness and Training	Securing Governments' Cyberspace	International Cooperation
Home Users/ Small Businesses		X	X		
Large Enterprises	X	X	X	X	X
Critical Sectors / Infrastructures	X	X	X	X	X
National Issues and Vulnerabilities	X	X	X	X	X
Global					X

Figure 9



Priority I
A National Cyberspace Security Response System

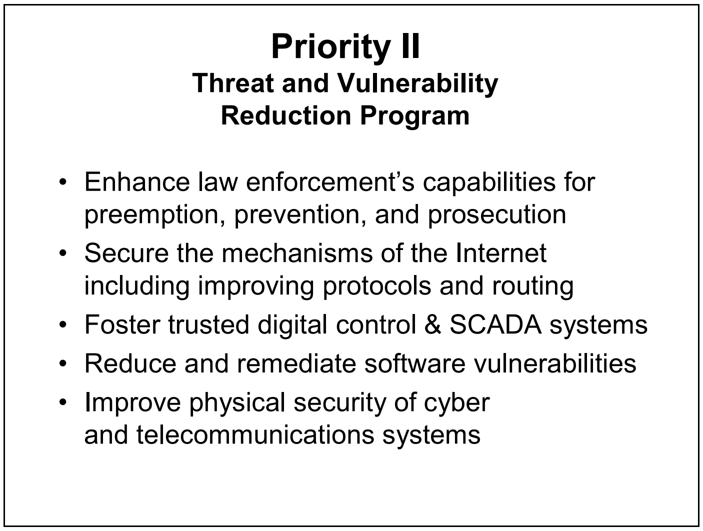
- Establish a public–private architecture for response
- Develop tactical and strategic analysis of cyber attacks and vulnerability assessment capabilities
- Encourage the development of a National Cyberspace Network Operations Center
- Expand CWIN to support DHS's security role in coordinating crisis management
- Exercise cyber security continuity plans

CWIN= Critical infrastructure Warning Information Network

Figure 10

of the things we did last fall was run a national cyber security exercise called Livewire. We need to mature our ability to cooperate in response, particularly against large-scale cyber events. We're learning.

Please read through the next figure (**Figure 11**). We started to have the discussion that there are a lot of places where the information infrastructure has vulnerabilities. These were our focal areas for remediation.



Priority II
Threat and Vulnerability Reduction Program

- Enhance law enforcement’s capabilities for preemption, prevention, and prosecution
- Secure the mechanisms of the Internet including improving protocols and routing
- Foster trusted digital control & SCADA systems
- Reduce and remediate software vulnerabilities
- Improve physical security of cyber and telecommunications systems

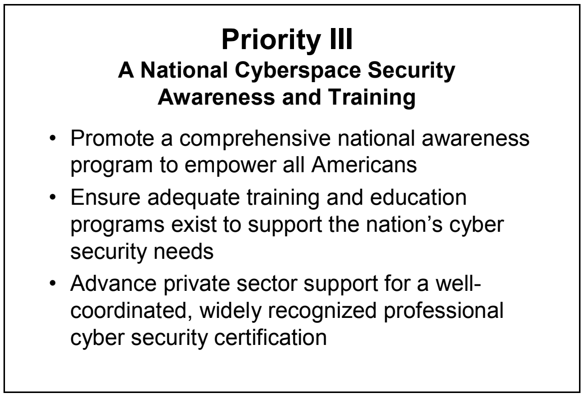
Figure 11

Student: I’ve heard stories about red-teaming our prevention capabilities: how American groups might go against government groups intentionally to see how far they can penetrate. Are we also gaming our response capabilities? If we have a response group, are we having them square off against guys in the Air Force whose job it is to mount an attack against cyber systems?

Rattray: This is actually the area where I’ve spent a lot of my energy in the last five years. In the Air Force we’ve conducted both red-teaming and exercises focused on our responsive capabilities. As I mentioned, last year we ran an exercise called Livewire, which was the first national cyber response exercise designed to mature the national cyber security response system. So we are starting to do that. Now, the Livewire exercise was basically notional injects. We didn’t have a live red team intruding into the electric power grid and the financial services sector and actually have defenders try to detect unauthorized or malicious activity. We’re a long way from having sufficiently developed approaches to do that sort of live play exercise, which is a challenge in terms of the understanding the strengths and weaknesses of our national cyber response system. So the first time we did it we basically said, “Here is a simulation of your infrastructure. Here are the events that are occurring. You tell us what your projected operational impact is. Would you talk to the government about this? When would you talk to the government? You guys in the government, what are you hearing from the private sector? How bad is it? Are we going to raise the homeland security alert level? If we do that, how are we going to explain it in terms of a cyber threat as opposed to terrorists blowing up bridges?”

I am a firm believer that you’ve got to try to put yourself through these exercise situations. Exercises and red-teaming are major ways forward to figure out how you respond to threats.

Awareness is an ongoing challenge (**Figure 12**). You are always going to have to educate people down to the individual user level about the fact that they’re in an environment that is shared by 300 million other users and some of those people are going to misuse those systems. Everybody from the individual up through the corporation has a role in protecting their portion of cyberspace. I don’t want to spend a lot of time on this. I think general awareness is well



Priority III

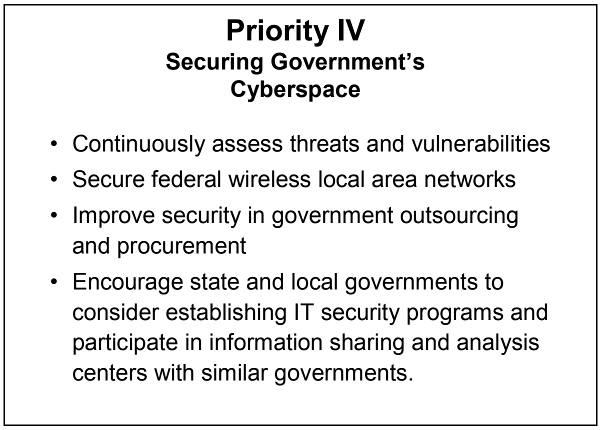
A National Cyberspace Security Awareness and Training

- Promote a comprehensive national awareness program to empower all Americans
- Ensure adequate training and education programs exist to support the nation's cyber security needs
- Advance private sector support for a well-coordinated, widely recognized professional cyber security certification

Figure 12

developed, but we have a continuing challenge to make sure that awareness remains high and everyone makes the appropriate effort to protect themselves.

The government should lead in securing its cyberspace (**Figure 13**). A recent evaluation by the Office of Management and Budget [OMB] gave the overall U.S. government information security posture a D. I'm going to take this discussion off on a tangent. The United States is the most self-critiquing culture you will see out there. The reason that we get better faster and are good at problem solving is that we are willing to give ourselves a D. I don't see many other governments grading the information security of their own organizations and giving them Ds. The United States is at least willing to admit that we've got flaws. I'll tell you, on the basis of my limited knowledge of how other governments work, this is actually a fundamental strength of our system. Everybody tries not to get a D the next time around. But we have a long way to go. That D was not completely ungrounded in terms of some of the reasons why that grade was handed out.



Priority IV

Securing Government's Cyberspace

- Continuously assess threats and vulnerabilities
- Secure federal wireless local area networks
- Improve security in government outsourcing and procurement
- Encourage state and local governments to consider establishing IT security programs and participate in information sharing and analysis centers with similar governments.

Figure 13

Student: Who within the OMB decides how to grade you?

Rattray: OMB has a really good set of information security metrics, largely developed by the National Institute for Standards and Technology [NIST], that they grade against. My concern with the metrics is that they are very much oriented to policy and organizational aspects of information security programs rather than evaluating operational capacity to protect systems. "Do you have a policy for this? Is this piece of technology in place?" You don't get a particular grade because a red team went in and said that compared to all the similar organizations they've examined you get an A if you're in the top 20 percent of the bell curve, a B if you're in the middle, a C if you're in the lower third, and a D if you're at the bottom.

As military officers, we go through different types of evaluations. In one sort, an IG [inspector general] comes in and goes through a checklist-based approach to whether you've done everything you were supposed to do to have a good information security program. It's useful but not sufficient. We always distinguish between these sorts of paperwork inspections and something called an operational readiness inspection, where a bunch of guys come in and watch you perform your mission: you go up and fly your airplane, or as an intel guy you give briefings to pilots about exercise intelligence you have received. Someone who is an expert in the field says "Yes, that was a good intel briefing" or "No, that wasn't a good intel briefing." The OMB evaluations are not operational readiness-type inspections.

This is my core set of concerns (**Figure 14**). I'd say we're doing better on the international cooperation front than on some of the three national security bullets. The State Department (and this is where personality is important) has a very experienced diplomat who is tenacious with the U.S. government as well as with her international partners and does a really good job of international outreach. We do a lot in working with other countries in this area. We just sent the Convention on Cybercrime to the U.S. Senate. It was written under the guise of the Council of Europe, but actually the United States wrote most of the content of the treaty.[8] We hope the Senate will recommend ratification of this treaty this year.

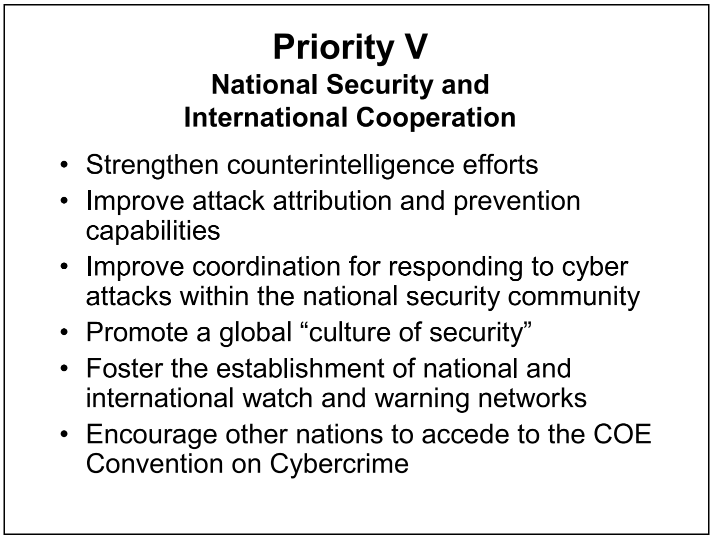
Student: In terms of international actors, how do you promote a global culture of security?

Rattray: One way we do it is through diplomacy. The United States led an effort in the United Nations General Assembly's Second Committee to issue a resolution recognizing the need for a global culture of security. We have bilateral meetings with other governments, including private sector participation on both sides.

Oettinger: It's another area where the private sector has an important role. If your bank does not adhere to certain standards, I'm not going to do business with you. If your Coca Cola bottling plant is not following certain practices to reduce the probability of some crud being injected into the sugar water, then I'm not going to license you.

Student: I guess what I'm wondering is if you see the cooperation that happened with international banking happening now with companies on security issues?

[8] Council of Europe, Convention on Cybercrime, 2001, [On-line]. URL: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/Convention/The_Convention.asp#TopOfPage (Last accessed on 19 December 2004.)



Priority V
National Security and International Cooperation

- Strengthen counterintelligence efforts
- Improve attack attribution and prevention capabilities
- Improve coordination for responding to cyber attacks within the national security community
- Promote a global "culture of security"
- Foster the establishment of national and international watch and warning networks
- Encourage other nations to accede to the COE Convention on Cybercrime

COE = Council of Europe

Figure 14

Rattray: The cybercrime treaty would probably be the most important practical measure. If we thought an incident were emanating from South Korea, and we and South Korea were both signatories to this treaty, South Korea would be under an obligation to have a 24/7 point of contact that the Justice Department could call up and say, "This bank is getting hacked. We believe it's emanating from this IP [Internet Protocol] address in South Korea. We request that you investigate." They would have an obligation to get back to us, and if it were a South Korean citizen they would either have to prosecute that person or extradite that person to the United States. So, to the extent to which your nation is fostering cyber security you should be willing to undertake this sort of step. It also has to do with harmonization of laws about what constitutes a cyber crime.

Student: We were talking previously about walls and how much security you want to put up so that there aren't these cyber attacks. In the context of terrorism there is a lot of discussion about security versus civil liberties. Do you have the same discussions happening in the world of cyber warfare? Is that a serious topic?

Rattray: It's a very serious topic. First among the threats we're concerned about would be non-state terrorist groups potentially using cyber means to conduct attacks. Where the balance with privacy actualizes itself is that we log a lot of activity on computer systems. Who is allowed to keep logs? There are limits. Tony and I were talking earlier today about what agencies can look at data that relates to U.S. citizens and under what conditions. This society jealously guards privacy. The extent of the authority of U.S. government agencies to identify who is hurting us and to use technological tools to gather information constitutes a very active portion of the debate.

The *National Strategy to Secure Cyberspace* has a statement that this will be done in accordance with the basic American commitment to privacy and civil liberties. I don't spend a ton of time on this. It's interesting in this society. So much is ingrained in us that while we debate with our lawyers about the interpretation of different laws we know that we're going to have to account for the privacy aspect of what we do in the government.

Oettinger: Let me just say that this gets complicated by some other factors that are not his responsibility. For instance, some European countries are much more stringent than we are about privacy and the motives are not always civil libertarian. The motive may be to introduce nontariff trade barriers to staunch the flow of outsourcing to the United States. We might want to do something like that if we get too exercised about outsourcing, so there is a trade dimension to this that makes it a very complicated problem.

Student: In terms of strengthening counterintelligence efforts, over lunch one of the things that you were talking about was the need to get companies to be more open about when they've been hacked so that information can be properly disseminated and companies can engage in the correct future actions. Companies don't have an incentive to do that now, because then they'll get dumped on by the market. Is there any way we could leverage our significant experience in information security to somehow create a community of IT [information technology] folks within these companies who have an institutionalized private access to information that won't get out of the IT departments? That way they can share among themselves and not worry about the investment departments dumping on them when they find out that Company X was hacked yesterday.

Rattray: There is a lot embedded in that. First, I don't think we should be so much seeking information from them as pushing out information to them about the characteristics of activity they really ought to be concerned about. Then the question becomes to whom we would push that information, which could get pretty sensitive if it were going to characterize espionage activity. How do we create that community of operators of critical systems so that the government can say, "Look, if you see this sort of activity, you ought to recognize that is significant. You ought to come back and tell everybody else what's going on in your network, and we prefer that you come to us."

Student: They're afraid that when they tell everybody the market is going to sock them.

Rattray: There are sharing mechanisms wholly outside the government in industry associations that depend on a degree of trust and recognition that nondisclosure is in their mutual interest. We need to create communities that cross the private sector–government barrier for the same sort of trust and information sharing. We have something called the National Security Information Exchange where there are nondisclosure agreements. Again, that's an area where lawyers get lots of employment. There are mechanisms that try to build that trust. I'll tell you: the trust often comes from face-to-face interaction. You can do a lot of paperwork that tries to create legal sanctions for breaking trust, but the way you create trust is by sitting in a room with somebody and having that person believe that you are credible and you won't share their information.

Oettinger: This is the first time in this conversation that trust has entered significantly, and it probably should have pervaded everything. Underneath all the technicalities, et cetera, nothing will work without reliance on trust. It's hard to overstate the importance of trust in everything we've been talking about.

Rattray: Yes, and I will tell you that this community is very technologically focused. They tend to want to create trust through technology implementations that prevent certain things from happening or assure you that there is authentication that the computer you talk to is being operated by the guy you think is operating it. My practical experience is that if it's public–private, you have to go to the CEO [chief executive officer] or the CSIO [chief security information officer] of the corporation and get those people to believe that if they give you information you're going to protect it properly.

Bob can talk to you at length about the Protected Critical Infrastructure Information Program. They have developed a system under the authorities of DHS to protect appropriate information disclosed about critical infrastructure from release under the Freedom of Information Act. That's a practical application of what you're talking about. It's so the private sector can come in and share information, but feel confident that the press or others can't get at it on the basis of the general government obligation to openness. There is a system now to protect certain types of information.

Oettinger: Again, this is where the U.S. Constitution becomes "trust but verify." There is no branch of the U.S. government and no part of the private sector that hasn't at one time or another broken that trust. Eternal vigilance is the price of establishing and maintaining trust.

Student: One private sector type of entity that does exist is what are called monitoring firms, which will monitor your network. They will, of course, have many clients, so that if one client is attacked the people monitoring your network are also going to be looking for the same thing on other networks. One of the CTOs [chief technology officers] regularly briefs these guys. I'm sure Bruce Schneier is someone you probably encounter a lot.[9]

Rattray: Those firms have an obligation not to disclose an attack to their other clients, but just to use the knowledge to further everybody's best interest.

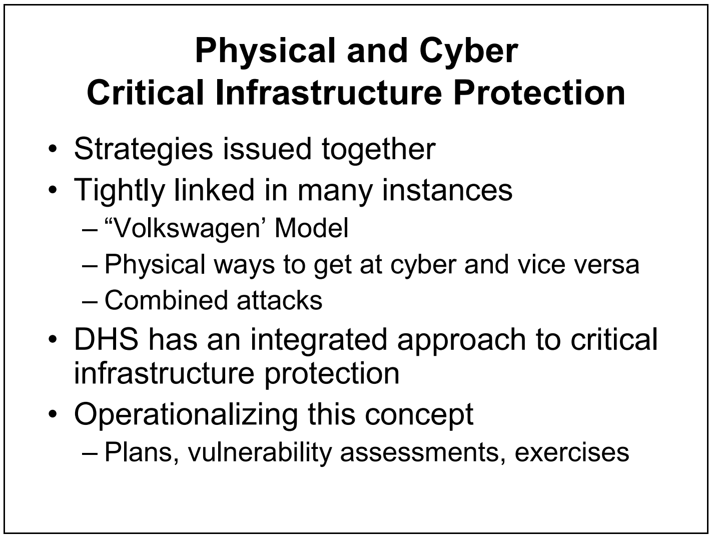
Student: They want to expand their business, so they have a very strong incentive not to reveal confidential information.

Oettinger: On the other hand, if they are owned by a foreign power they might at some point just do that.

Rattray: Foreign ownership and the risk posed by different types of foreign influence for different IT enterprises is a topic of much discussion with the U.S. government. There are very different perspectives on how we should diminish those risks. There are blunt things we can do. There are technologically focused solutions that we might implement. Globalization poses a very rich set of issues.

We've talked enough about this (**Figure 15**). Down at the bottom it mentions exercises. A fundamental thing that I would assert is that your organization may believe that it has a good technological laydown in terms of protective measures, that it has good plans and policies in place so that those technologies are used properly, and that users in your corporation or your

[9] Bruce Schneier is the founder and CTO of Counterpane Internet Security, Inc.



Physical and Cyber Critical Infrastructure Protection

- Strategies issued together
- Tightly linked in many instances
  - “Volkswagen’ Model
  - Physical ways to get at cyber and vice versa
  - Combined attacks
- DHS has an integrated approach to critical infrastructure protection
- Operationalizing this concept
  - Plans, vulnerability assessments, exercises

Figure 15

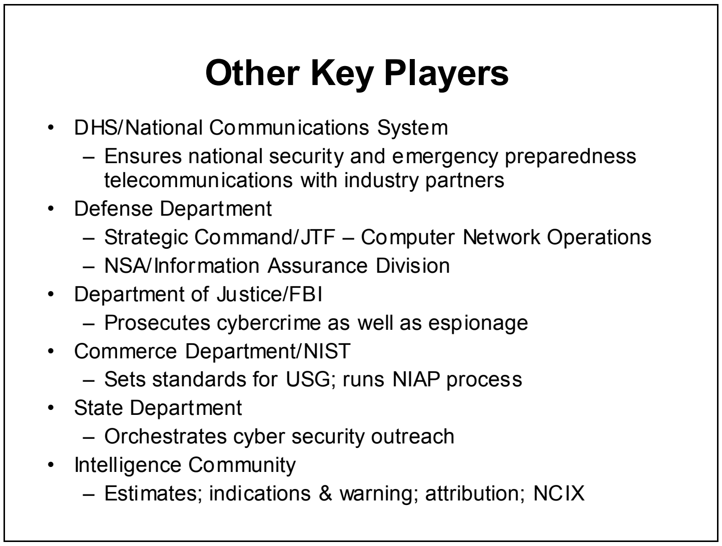
government agency don’t do the wrong things in your system. I will tell you that the best way to test that is to have somebody come in and try actually to penetrate your system.

I want to get back to exercises. I’m going to get back to red-teaming and the significance of that, given what I think are some fundamental characteristics of where we’re at in information infrastructures and the technology.

As I mentioned earlier, DHS heads several initiatives in this area (see Fig. 5), but while DHS is the national lead for doing things that relate to securing cyberspace, they cooperate with a whole bunch of other organizations who operate under other authorities to perform other very significant tasks (**Figure 16**). We’ve got something called the National Communications System [NCS], which is also in the DHS now. It used to be in the DOD. The NCS reaches out to industry and makes sure that government communications survive attack: that the president can talk to his department heads in the case of a national emergency, that our military command and control works, and that we can reach out to our embassies around the world. So they have a critical role.

The DOD has shifted responsibility for cyber security of its networks to an organization named Strategic Command, which has a Joint Task Force for Computer Network Operations focused on protecting the DOD information systems. They have access to some very sophisticated resources, so they help other government agencies in terms of understanding what might be happening out there, especially if it’s a cross-government attack.

The NSA has a protective mission in addition to its intelligence-gathering mission; the organization that does this, the Information Assurance Directorate, is a national resource. It has authority to assist others outside the DOD.



Other Key Players

- DHS/National Communications System
  - – Ensures national security and emergency preparedness telecommunications with industry partners
- Defense Department
  - – Strategic Command/JTF – Computer Network Operations
  - – NSA/Information Assurance Division
- Department of Justice/FBI
  - – Prosecutes cybercrime as well as espionage
- Commerce Department/NIST
  - – Sets standards for USG; runs NIAP process
- State Department
  - – Orchestrates cyber security outreach
- Intelligence Community
  - – Estimates; indications & warning; attribution; NCIX

NCIX = National Counterintelligence Executive NIAP = National Information Assurance Partnership

Figure 16

Oettinger: If anybody's interested, some of the directors of the NSA section concerned with the protection of information have spoken to this seminar over the years: Harold Daniels and Jim Hearn.[10] So if you're interested in that end of the world, take a look at the publications of the seminar on the PIRP Web site.

Rattray: The Justice Department and the FBI are at the pointy end of the spear in many ways when we have an incident. The first thing that happens when computers get hacked into is that law enforcement must determine what happened and if a crime was committed. If an intruder has violated the computer crime laws, which are pretty broad, and has achieved unauthorized access or inflicted a fairly low level of economic damage, the FBI and others have the authority to go out and investigate.

The Commerce Department runs the NIST, which sets standards for nonclassified government systems, and something called the National Information Assurance Partnership [NIAP]. NIAP is the process by which private laboratories validate that certain products perform as advertised in a security sense. I talked about the State Department, and the intelligence community clearly plays a role. It's not one government agency, and therefore, ensuring that there are coordination and a common response, particularly in situations that are complex and engage different government agencies' authorities, is a continuing challenge.

[10] Harold Daniels, "The Role of the National Security Agency in Command, Control, and Communications," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1986* (Cambridge, Mass: Harvard University Program on Information Resources Policy, I-87-1, February 1987), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=272 ; and James J. Hearn, "Information System Security," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1992* (Cambridge, Mass: Harvard University Program on Information Resources Policy, I-94-4, August 1994), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=215

Oettinger: You might ask, "Why are we so lunatic as to spread this all over the place?" Some of it registers as bureaucratic nonsense, but some of it is profoundly political and indeed constitutional. The reason for dividing this sort of standard-setting thing between the Commerce Department and NSA again has to do with distrust of one part of the government as opposed to the other. You can go back to the Carter administration and you will find during that period enormous debates over who should have that responsibility. The compromise ultimately was reflected in this. Nobody wanted to entrust the whole enchilada to a single agency.

Rattray: President Reagan gave it in a presidential directive primarily to the NSA alone, and the next year Congress came back and said "No, we're going to split it, because we shouldn't invest the NSA alone with the responsibility." In a post-9/11 environment, and given the more robust resources of NSA, we need potentially to draw on that resource. That gets back to the privacy concern operating here: that intelligence agencies are less trusted by the American people to protect privacy than the Commerce Department is.

So Tony's point is well taken. The president couldn't put this in a single place even if he wanted to, plus there is value to splitting it. The State Department is better at getting a dialogue going with the other governments and international governmental organizations about cyber security than the DHS is. What the State Department needs is for the DHS to tell the State Department what we need from the Koreans in terms of cyber security. This interagency coordination is actually at the core of what the NSC and the HSC do to make sure that everybody is playing well with everybody else in an effective fashion.

NCIX, the National Counterintelligence Executive, is an organization that is only a few years old. It is supposed to develop the national strategies for dealing with things such as espionage in cyberspace.

Oettinger: The head of it is a lawyer named Michelle Van Cleave, who came before this seminar a couple of times wearing other hats.[11]

Student: To what degree is the complexity of this whole domain a kind of defense? What I mean is that there are all these scary vulnerabilities that you talked about. In your book you also pointed out that we live with a high degree of static. Networks go down all the time; servers collapse; there's all the spam coming in. There is such a high degree of friction that I could imagine that some deliberate attacks could really get lost in the everyday noise of cyberspace.

Rattray: This is one of the fundamental things that the book lays out and that still plagues our understanding. We do not know whether complexity is bad because complex interrelationships create negative cascading effects or whether complexity is good because the system has robustness for adaptation and redundancy. It's also hard for attackers to project the effects they're

[11] Michelle Van Cleave, "Intelligence: The Science and Technology Connection," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1993* (Cambridge, Mass: Harvard University Program on Information Resources Policy, I-94-5, August 1994), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=292 ; and "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/publications/pdf-blurb.asp?id=434

going to have on the system, because they have a hard time discerning how everything is hooked together and what backup mechanisms exist. It's a challenge that will have to involve academe to get a deeper understanding, because it's going to require deep thinking and multiyear research to understand the implications of complexity for this dynamic. I remain agnostic about whether complexity is more good than bad.

Oettinger: To put that in concrete terms, there is a very simple example that comes out of the space program. Redundancy is nice, because if one unit fails the other unit will be working. But there is a tendency to make the redundant unit identical in design to the original unit, so the conditions that make the first one fail will likely make the second one fail. However, if you build the two of them differently there's diversity as well as redundancy. As the system gets more complicated, this homely, simple-minded example gets humongously complicated and it's extremely difficult to net out whether redundancy or diversity really gives you greater or lesser security.

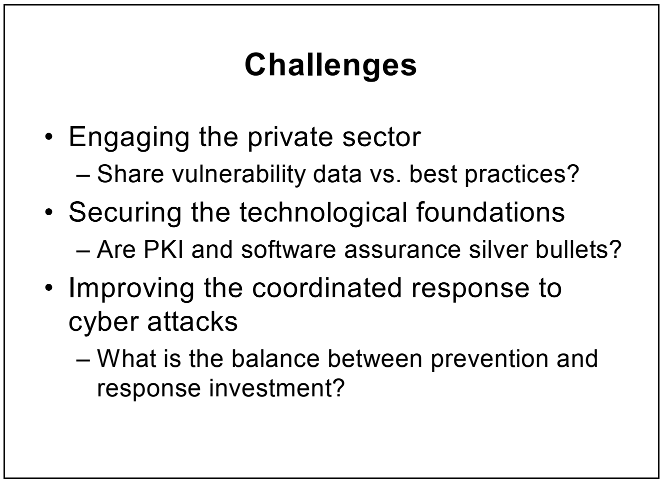
Rattray: In practice, banks feel an obligation to have diversity of service providers. If suddenly Verizon doesn't work they are backed up by AT&T. What the finance sector didn't have visibility into until a recent study was that Verizon and AT&T both put their circuits down the same wire, which ran under one bridge. So if you take out a bridge in a place like Manhattan—and there is only a limited number of bridges out of Manhattan—no matter how much contracted diversity you have, you still have only a limited number of vulnerabilities. Those sorts of things through the infrastructure remain pretty opaque. The benefit of it is that they're also always changing. Attackers not only have to understand it once but also have to continue to understand it, which is going to require a level of ongoing investment in understanding what vulnerabilities you have that are going to hurt you.

Oettinger: A screwed-up system is hard for the other guy to decipher, too.

Rattray: We talked about the private sector (**Figure 17**). I'll tell you that I think the technological foundations will remain weak for the indefinite future. The 1991 *Computers at Risk* report basically identified the economic dynamics that make that the case. The dynamics haven't changed. I could argue they are actually getting worse. The people who sell security products, and information security technology specialists, talk about public key infrastructures [PKI] and analytic tools that will allow us to analyze millions of lines of code and find programming errors or malicious code. My gut feeling as a non-technologist is that those will not be silver bullets. They will not provide the robustness to the information infrastructure over time that some of their proponents believe.

Oettinger: They're also highly vulnerable to somebody selling out. The history of cryptography by and large is that somebody sold the code for ideological or for financial reasons, and any of these things are vulnerable to that.

Rattray: Right. You see in cyber security area a lot of "Yes, it's bad now, but if we invest in this technological area—encryption or software assurance—we will be able to make many of the things that cause vulnerability now go away." You have to form an opinion on that. Mine tends to be fairly skeptical.



Challenges

- Engaging the private sector
  - Share vulnerability data vs. best practices?
- Securing the technological foundations
  - Are PKI and software assurance silver bullets?
- Improving the coordinated response to cyber attacks
  - What is the balance between prevention and response investment?

Figure 17

Student: I feel I should just respond to Tony's comment. One of the really positive things the security community that came up with public key cryptography did was develop Kirchoff's Law, which said that when you develop a crypto system, you should assume that the attacker knows everything about how this system works except for the key.[12] Yes, the key can still be sold, but this was a huge advance, because it said "You're going to be moving your eggs to this one basket, but at least you will know something about the other baskets." Until then a lot of people said "Just make it so complicated so that nobody can understand it."

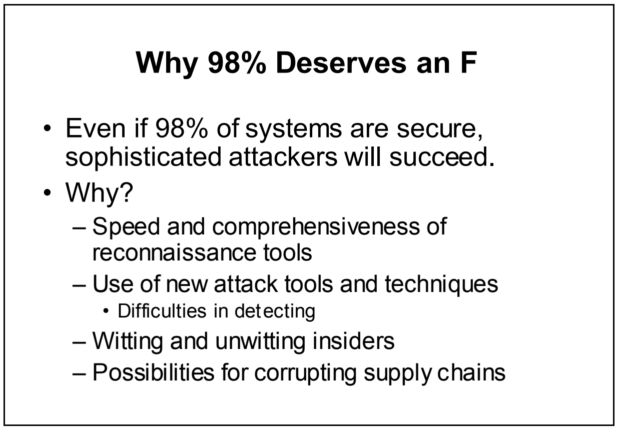
Rattray: My concern about PKI systems is with the implementation. Unless they are very easy for users to implement, to include the data they store as well as communications as they transit, people won't use them, because they won't perceive that the security they gain is worth the hassle. In aggregate, their vulnerability can become the door through which a much more serious set of vulnerabilities is created.

Student: I'm not sure I agree, because I think a lot of companies right now think that cyber security is going to hamper the progression of some technologies. For example, Bill Gates often mentions that the main chance for Microsoft to create a new product is basically for security. It seems that new technology, like trusted chips and that kind of thing, could go a long way toward doing that. I was looking at a research report and their vulnerabilities actually diminished between 2002 and 2003. Is there any data on that?

Rattray: This is a good lead in to the next slide.

When red teams or penetration assessment teams have done their business over the last five years, more and more of the systems that they go after are secure (**Figure 18**). If in 1998 50 percent of the systems that a red team looked at were secure, now it might be 98 percent. I've worked a lot with red teams. I will argue that is insignificant. Once you get into a network and

[12] Kirchoff's Law is "All security rests in the key."



Why 98% Deserves an F

- Even if 98% of systems are secure, sophisticated attackers will succeed.
- Why?
  - – Speed and comprehensiveness of reconnaissance tools
  - – Use of new attack tools and techniques
    - Difficulties in detecting
  - – Witting and unwitting insiders
  - – Possibilities for corrupting supply chains

Figure 18

you gain control and basic privileges on a system that is trusted by the other computers in that system, you're cooked.

Now, that's overly simplistic. You can do a lot of internal auditing. You can look for an insider in your network. You can assume you have an insider, but then you have to secure every computer against every other computer to the level that you have at the outside of your enterprise boundary. That gets to be very expensive and the sophisticated guys can generally go right through firewalls once they've got a control of a system on the inside of a network.

I don't want to get too technical here, but the computers have to have some ability to communicate with each other or your network has no value. So if sophisticated attackers can make their communications look like communications that are supposed to occur on the network, which is pretty easy to do once they're inside your system, you've got a big problem. If we're talking about a guy who has years and can wait and do this slowly and basically leverage more and more access, he can find out more and more about the significance of the computers that he's in, take information out, and understand which computers are core to the function of the network and which networks are core to the function of the organization using them.

So what I'm concerned about in the security community (and I heard Steve Ballmer, Microsoft's CEO, talk last week about their security) is that they're still thinking about building better walls. You can debate what I'm about to say, but security devices will have to get nearly perfect before you can keep a sophisticated adversary out, and once he's in you have a big problem. The security community is not thinking enough about the insider threat yet. They're not thinking about how to react when the system is compromised, let alone about the guy who walks in and tries to screw your network up because he's the agent of the guy who is attacking you. So that's why I have skepticism on the basis of my experience in trying to understand the threats that I'm concerned about: state espionage programs, sophisticated non-state actors, or state actors intent on disruptive activities.

I'm less concerned about kiddie hackers and low-level fraud and crime. It's not that we shouldn't be attentive to those, or that Steve Ballmer and others at Microsoft shouldn't be building more secure computers, or that cryptography shouldn't be in place so that you're confident that your eBay transaction is safe. But in terms of my national security threat, those sorts of security approaches are going to have a limited impact. Does that make sense? I put that case polemically, but from where I sit after ten years of looking at this problem we still focus too much on finding a technological holy grail.

Oettinger: We want to thank you very much. Here's a small token of our large appreciation for you.

Acronyms

CEO	chief executive officer
CERT	computer emergency response team
CTO	chief technology officer
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
HSC	Homeland Security Council
HSPD	Homeland Security Policy Directive
IT	information technology
NCS	National Communications System
NCSD	National Cyber Security Division (DHS)
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NRC	National Research Council
NSA	National Security Agency
NSC	National Security Council
OMB	Office of Management and Budget
PKI	public key infrastructure
SANS	SysAdmin, Audit, Network, Security
SCADA	supervisory control and data acquisition
USAF	U.S. Air Force
Y2K	Year 2000

Seminar2004

ISBN 1-879716-89-5