no specialty in the computer career fields for network administrators, computer security personnel, nor in the criminal investigative career field for computer crime investigators.

In order to ensure that computer security positions are filled with personnel that possess the requisite experience and training the Staff recommends the creation of a Government Computer Security Specialist Career Field that will include potential for career progression and incorporate specialized computer security training.

In order to promote a stable pool of information security managers within the U.S. government, the Staff recommends the creation of a Government Computer Systems Administrator Career Field that will include potential for career progression and incorporate specialized computer security training.

In order to promote and improve our government's computer crime investigative potential, the Staff recommends the creation of a Government Computer Crime Investigators Career Field that will include the potential for career progression and specialized computer crime investigation training.

Vulnerability testing and assessment of government and government interest computer systems is the best method of enhancing awareness of the vulnerabilities of our information infrastructure. Presently, only the Defense Department has an aggressive vulnerability program.

The Staff recommends that the federal government promote regular vulnerability assessments, or ''red teaming,'' of government agencies, especially agencies outside of the Department of Defense. The Staff further recommends that an agency be designated to perform such vulnerability assessments in the same manner that the Defense Information Systems Agency (DISA) perform such assessments for the armed services.

One of the most significant voids in computer security is the lack of reporting of attempted and even successful penetrations of government systems as well as other systems of national interest. Mandating the reporting of intrusions in government systems will foster a greater security culture with the NII. Further, it is important to give private industry a mechanism within which it can report intrusions without fear of inciting customer insecurity.

The Staff recommends that the U.S. government mandate the reporting of intrusions and attempted intrusions in all government and government interest systems. The Staff further recommends that federal agencies develop protocols and procedures for reporting computer intrusions, and subsequent referral of same to proper criminal or other appropriate agencies like the proposed National Information Infrastructure Threat Center.

The Staff further recommends that the federal government encourage private industry and the private sector to report intrusions into private information systems. The Staff would further recommend that the government promote private industry reporting through creation of anonymous clearinghouses or similar methods.

Logon warning banners that advise users of government computers that there is no expectation of privacy, though recommended by the Department of Justice, are not mandatory on government computer networks. The logon banners put users on notice that they have no reasonable expectation of privacy on government systems and the use of the system constitutes consent to monitoring. Presently, when intrusions occur on government systems, lack of such a logon banner hampers investigative efforts and response.

The Staff recommends logon warning banners become mandatory for all government and government interest systems.●

NATIONAL SECURITY AND THE INFORMATION AGE

● Mr. NUNN. Mr. President, technology has long been an instrument of power and change. From the invention of the printing press to the advent of the industrial revolution to the development of nuclear weapons, technological advances have profoundly altered our society and changed the course of our history. Today, we find ourselves in the midst of one of the most far-reaching technological developments of all—the information age.

OUR INFORMATION INFRASTRUCTURE

Advances in computing and networking have affected every aspect of our society—from civilian government and the military, to public utilities, health care, communications, transportation, and financial systems. Computer networks and the ever-increasing power of the information systems they connect, are compressing time and space, creating vast efficiencies in the delivery of goods and services. Government is more productive and connected, business is more robust, versatile, and cost-effective, and individuals now have access to large caches of information and each other.

The rush to connect seems to reach new and unimaginable heights each day with the announcement of a more powerful computer or some new innovation. Just 5 years ago the number of users on the Internet totaled 2 to 3 million. Today, over 55 million log-on worldwide and the number grows. Computer links that stretch around the world transcend national and regional boundaries: Beijing and Baltimore are within a keystroke of each other. Equally impressive is the expanding technology that supports this revolution. Today's home computers are literally hundreds of times more powerful and versatile than the mainframe systems that NASA used to send a man to the moon. Connectivity between networks has similarly increased: In 1980, most modems required nearly 3 hours to transmit a 200 page book; today's commercially available modems can transmit the same book in 0.06 of a second.

Along with the great promise of the information age, however, has arrived new dependencies. Our banking and financial systems, though more efficient, rely almost totally upon daily electronic fund transfers in excess of $1 trillion. Our transportation system—air, rail, and road—is able to receive and analyze vast amounts of data but must also be certain of the accuracy of the information directing its critical operations. Energy and communication networks are more responsive but are similarly reliant upon the redundancy of electronic networks. And the information revolution in military affairs, though establishing the unquestionable preeminence of our force structure, has fostered a dependency upon 2 million interconnected DOD computers.

How would we get by if the information infrastructure of any of these critical systems proved unreliable?

As we rush to connect to the information superhighway, are we sufficiently addressing the potential weaknesses created by our growing dependency on computers and networks? To what extent can the vital services supported by our information infrastructure be disrupted? How can we be assured that the information stored—especially data related to our national security—retains its availability, reliability, and confidentiality?

THE THREAT FROM CYBERSPACE

Ironically, the same technological advances that have brought us the advantages of the information age, have also given us the tools to disrupt and exploit it. In the early 1980's only the very technically competent had the expertise to break into computer systems. Not only were there fewer hackers, there were not as many targets.

Today, the situation is reversed: while the hacker tools are becoming more sophisticated, they are also becoming more available and user-friendly, requiring little expertise. Logic bombs, viruses, password sniffers and other tools that can disrupt and destroy computer networks, are now widely available on the Internet. For instance, last year ''point and click'' computer security program—Security Administrator Tool for Analyzing Networks or ''SATAN''—was disseminated on the Internet. Now this computer program, which provides its user with automated intrusion capability into many networks, is available to millions.

In hearings of the Permanent Subcommittee on Investigations earlier this year experts demonstrated how many of our critical computer networks were neither secure nor confidential. A report issued this year by the General Accounting Office estimated that the unclassified but sensitive networks at the Defense Department are likely experiencing as many as 250,000 computer attacks per year. Vulnerability studies of DOD networks suggest that these network attacks could be successful more than 65 percent of the time. Over 90 percent of all Department of Defense voice and data traffic transits these networks, and the data includes sensitive research data and valuable intelligence information. Furthermore, these systems support critical defense missions related to troop movement and operational plans, procurement, and weapons systems maintenance.

Statistics from the civilian area are equally troubling. A recent FBI survey that included corporations, financial institutions, universities, and health care institutions revealed that 42 percent of those responding experienced

some form of intrusion or other unauthorized use of computer systems within the previous 12 months. Over 15 percent of these attacks involved the unauthorized altering of data.

We have already observed anecdotal evidence of this threat. Last year two London residents penetrated the Rome Air Development Center computers at Griffiss Air Force Base in New York. Earlier this year an Argentinean national attacked NASA and other DOD computer systems from his living room in Buenos Aires. Recently, a computer gang based in St. Petersburg, Russia, launched a computer attack against Citibank and were discovered only after they were able to steal millions. Though disturbing, these incidents involved the least competent and immature attacker. The more sophisticated and structured attack likely occurs without detection or apprehension.

Fortunately, we have not suffered serious breakdowns in our information infrastructure. Americans have not had to endure an unexpected, prolonged, and widespread interruption of power, the indefinite grounding of air traffic, or the loss of banking and financial services and records. We should not, however, wait for an ''electronic Pearl Harbor'' to spur us into rethinking the speed and nature of our entry into some of these information technologies.

Our intelligence agencies have already acknowledged that potential adversaries throughout the world are developing a body of knowledge about Defense Department and other government computer networks. According to DOD officials, these potential adversaries are developing attack methods that include sophisticated computer viruses and automated attack routines which allow them to launch anonymous attacks from anywhere in the world.

In testimony before the Permanent Subcommittee on Investigations this year, CIA Director John Deutch explained that both hostile nations and terrorist organizations can, with relative ease, acquire the techniques to penetrate information systems. Indeed, in response to a question as to where he would place the threat of cyber-based attacks in terms of overall threats to the United States, Director Deutch stated as follows:

> I would say it is very, very close to the top, especially if you ask me to look 10 years down the road. I would say that after the threats from weapons of mass destruction . . . nuclear, chemical and biological weapons, this would fall right under it; it is right next in priority, and it is a subject that is going to be with us for a long time.

A DIFFICULT PROBLEM FOR GOVERNMENT

Who is the enemy and what does he or she want? Is it a lone anarchist trying to create chaos, or a well-organized group sponsored by a foreign government? Is the motive of the bad actor greed, espionage, or vandalism? Notwithstanding Director Deutch's admonitions, the staff of the subcommittee found that the collection and analysis of data that would help provide the nature and extent of the threat posed to our information infrastructure is not presently enough of a priority of our intelligence community. The Brown Commission Report on Roles and Capabilities of the United States Intelligence Community similarly observed that the activity that was occurring did ''not appear well coordinated or responsive to an overall strategy.''

Likewise, the law enforcement community has been unable to provide reliable threat assessment in this area, perhaps because so little is ever reported to law enforcement. According to an FBI survey, only 17 percent of those responding indicated that they would advise law enforcement if attacked.

Without reliable threat assessment data we can neither conduct meaningful risk management, nor structure a coherent national response to this issue. This is one area where we cannot afford to be operating in the dark. Too many parts of our society have come to rely on the information infrastructure for us to remain ignorant of the extent of our vulnerabilities and the nature of the threat facing us.

This issue poses problems for our Government that are not easily addressed within the framework of our traditional national security strategies. Historically, our Government's security threats have been defined geographically: a foreign threat versus domestic. And the type of threat would inspire a different response from the appropriate agency; whether enforcement, military or intelligence. When we move from the physical world into cyberspace, traditional divisions of responsibility, and assignment of roles and missions become confusing. Is the bad actor a 16 year old, a foreign agent, an anarchist, or a combination thereof? Furthermore, the Internet exists in a ''border less'' world. How do you ascertain the nature of a threat if you don't know the motive of your adversary? Which agency is used if you can't tell until the end of the investigation the origin of the attack?

CONNECTION, PROTECTION AND A CULTURE OF SECURITY

I believe if we fail to recognize and address the potential vulnerabilities of our information infrastructure today, we may find ourselves victims to very costly scenarios tomorrow. Security must be imbedded into not only the technology of the computer age, but its culture as well. Computer users, systems administrators and software and hardware manufacturers must emphasize security on the front-end, not as an afterthought.

Many critical elements of our infrastructure—power, communications, financial, transportation—are largely in the hands of the private sector. As these critical elements become more reliant upon open computer networks, government will have to partner with industry to ensure the reliability of the systems they support. Our intelligence and law enforcement agencies must develop reliable threat estimates that will not only help secure government and military systems, but provide data to the private sector so that they can manage their own attendant risks. Pivotal to this challenge will be fostering trust between industry and government in this arena.

Finally, we must be willing to reconsider our previously defined notions of national security. The threat from cyberspace, because it can emanate from a borderless world that transcends national boundaries, eludes many of our traditional national security assets. We cannot permit this problem to get lost in the seams of our intelligence, enforcement and defense communities. We will undoubtedly require the types of international alliances that has served us well in our defense of our physical perimeters.

This year the minority staff of the Permanent Subcommittee on Investigations completed a lengthy investigation into these issues that included a report entitled ''*Security in Cyberspace*.'' The report set forth numerous recommendations intended to improve our Nation's cyber defenses. Those recommendations include some key proposals:

(1) Formulate a national policy that promotes the security of our information infrastructure;

(2) Create a National Information Infrastructure Threat Center that includes the law enforcement, intelligence, and the defense communities as well as liaison with the private sector;

(3) Complete an intelligence estimate of the threats to our information infrastructure, that includes an unclassified version that can be made available to the private sector;

(4) Promote the creation of an international computer crime bureau with emergency response capability;

(5) Maintain a better and qualified pool of computer security professionals and, generally, improve the security consciousness of our government's users and managers;

(6) Promote regular computer vulnerability assessments, or ''red teaming'' of government agencies, especially agencies outside of the Defense Department; and

(7) Encourage better reporting of computer incidents within private industry while creating a mechanism within which industry can report intrusions without fear of inciting customer insecurity.

Ultimately, there is no question that the information age will bring us to new plateaus that will greatly benefit our citizens and our world. We must make sure, however, that in our rush to connect, we do not lose sight of the more mundane but equally important need to protect.●

TERRORISM MEETS PROLIFERATION: THE CONVERGENCE OF THREATS IN THE POST COLD WAR ERA

WHEN FICTION BECOMES REALITY

● Mr. NUNN. Mr. President, last year, I spoke to a group about the changes that have occurred since the demise of