Committee's Subcommittee on Oversight. Frankly, I was shocked to find that the Department had not yet done their own study of this potentially huge future liability, and that is why I introduced this amendment.

It is vital that the Department of Energy obtain comprehensive and accurate information regarding the extent and valuation of natural resource damages at DOE sites. This is especially important if we are to make realistic budget assumptions today and set realistic budget goals for the future. Unfortunately, there has not been a reliable study done on this issue to date.

During the course of Superfund hearings held in the Environment and Public Works Committee, significant questions have been raised about the Department of Energy's liability for natural resource damages at their Superfund sites. Department officials first estimated liability in the hundreds of billions of dollars. Since that time, GAO has looked at the situation, as has CEQ. However, the CEQ and GAO estimates are quite different. GAO estimates a high range of $15 billion while CEQ says the high range is $500 million. The disparity between these two studies is troubling, as is the fact that DOE has never done their own study.

This amendment directs DOE to conduct their own study, to use realistic assumptions about liability based on the real world experience private parties have already had, and to report to the Congress 90 days after enactment. This real world experience is the methods in the current natural resource damages assessment regulations, and should be consistent with the position asserted by public trustees in suits against private parties and with the position supported by the administration pertaining to damages against private parties. While I would be happy to work with DOE to ensure they have enough time to do a credible job, it is important that they complete their work before we move to reauthorize the Superfund program next year and before next year's appropriations cycle.

Finally, I want to emphasize that the intent of this section is purely for oversight functions. This section in no way should be interpreted as a reflection of support for the current operation of the natural resource damages provisions of CERCLA. I in no way endorse the methodologies used by public trustees under the current natural resource damages regulations. I simply believe that if private parties face these regulations today, and if the Department of Energy is the single largest potentially responsible party in the country, then we ought to use the same standard in estimating DOE liability at these sites. I look forward to receiving this study and to possible future hearings on this issue.

Mr. President, I want to thank Chairman THURMOND and Senator NUNN for their help on this matter.

CABLE TELEVISION PROVISION

Mr. SMITH. I would like to engage the chairman and ranking member of the Senate Armed Services Committee on section 833 of the conference bill, relating to cable television franchise agreements on military bases. That section implements an advisory opinion of the U.S. Court of Federal Claims, which found that cable television franchise agreements on military bases are contracts subject to the Federal Acquisition Regulation [FAR].

As chairman of the Acquisition and Technology Subcommittee, I believe that when negotiating the settlement ordered by section 833(3), the parties should give due consideration to the fair compensation of cable operators terminated for the convenience of the Government in accordance with part 49 of the FAR. Factors to be considered may include, to the extent provided in the FAR, interest on capital expenditures, settlement preparation costs, and other expenses reasonably incurred by such operators in connection with constructing their cable systems or obtaining fair compensation.

Mr. THURMOND. I agree with the statement of the Senator from New Hampshire.

Mr. NUNN. I also agree with the statement of the Senator from New Hampshire.

SUBMARINE LANGUAGE

Mr. LIEBERMAN. Mr. President, in section 121 of the conference report I read that funds in this bill are:

"* * *available for contracts with Electric Boat Division and Newport News Shipbuilding to carry out the provisions of the "Memorandum of Agreement among the Department of the Navy, Electric Boat Corporation (EB) and Newport News Shipbuilding and Drydock Company (NNS) concerning the New Attack Submarine" dated April 5, 1996, relating to design data transfer, design improvements, integrated process teams, and update design base.

Further, in the bill, under subsection (g) Design Responsibility, I read,

The Secretary shall ensure that both shipbuilders have full and open access to all design data concerning the design of the submarine previously designated by the Navy as the New Attack Submarine.

Mr. President, reading a portion of the aforementioned memorandum of agreement, a copy of which I am submitting for the record, NNS is to "be provided design deliverable information in a manner and scope that is generally consistent with that provided in the latest submarine program (SeaWolf). Design data transfer will be conducted in the most cost effective manner to support construction of follow-on ships at NNS." My interpretation of subsection (g)(1) of section 121 is that this subsection does not require the transfer of any design data between the shipyards which are not required by the memorandum of agreement. Am I correct in my interpretation of the intent of the conferees?

Mr. COHEN. Mr. President, I would say that the Senator from Connecticut is correct in his interpretation of the language in the bill regarding the transfer of design data between the two shipyards. It was the intent of the conferees to reaffirm last year's requirement requiring the transfer of design data regarding the new attack submarine to Newport News Shipbuilding. It was not the intent of the conferees to change the terms of the memorandum of agreement. Further, it was the intent of the conferees that the appropriate US Navy official resolve differences of opinion about what information is required to be transferred under the MOA.

Mr. KENNEDY. Mr. President, may I say that I fully agree with the distinguished chairman of the Seapower Subcommittee on this point.

Mr. WARNER. Mr. President, I agree with my colleagues interpretation of this important subsection of the conference report.

Mr. LIEBERMAN. Mr. President, thank you for providing me the opportunity to clarify this most important section of the conference report.

NUNN-LUGAR-DOMENICI DEFENSE AGAINST WEAPONS OF MASS DESTRUCTION

Mr. NUNN. Mr. President, after a truly heroic effort by both members and staff, before the recess we completed action on a conference agreement on the fiscal year 1997 Defense authorization bill. I hope this agreement will be voted on by the Senate soon. I wanted to take a few moments to highlight one provision in that bill which relates specifically to a recent tragic incident that has hit all of us in our hearts and homes. The incident to which I refer is the terrorist pipe bomb that went off in Centennial Park—the heart of the Olympic celebration in Atlanta—in July, which killed 1, caused the death of another, and injured over 100 people.

But, Mr. President, at this point in history, we have to ask ourselves, "What if?" What if this hadn't been a crude pipe bomb? What if the individual who planted this terrorist device had used information readily available on the Internet and materials readily and legally available to concoct a chemical weapon? Or, worse, suppose he had concocted a biological weapon?

The answer seems too terrible to consider, but consider it we must. And that is precisely why Senator LUGAR, Senator DOMENICI, and I cosponsored the Defense Against Weapons of Mass Destruction Act, an amendment—adopted by a unanimous vote in the Senate—to the Defense authorization bill that addresses this very threat. I am pleased to say that our colleagues in the House of Representatives also accepted this amendment in the conference report virtually as it passed the Senate.

Mr. President, the Defense Against Weapons of Mass Destruction Program, now title XIV of the Defense authorization bill, provides $201 million—$144 million to the Department of Defense and $57 million to the Department of

Energy—to address the threat of proliferation of weapons of mass destruction.

DOD is being given $65 million to conduct a program to train, equip, and assist local first responders in dealing with incidents involving nuclear, chemical, and biological weapons and related materials; $10.5 million of this funding is specifically earmarked for DOD assistance to the Secretary of Health and Human Services in forming emergency medical response teams capable of dealing with these materials.

DOD is also being given $30 million both to provide equipment and assistance to the United States Customs Service and to help train customs services in the former Soviet Union, the Baltic States, and Eastern Europe in an effort to improve our ability to detect and interdict these materials before they reach the hands of terrorists in the United States. An additional $27 million is provided to DOD and DOE for research and development of improved detection technologies, which are badly needed.

Finally, DOD and DOE are provided additional funding to address the threat of proliferation at its source. In addition to being fully funded at the administration's request of $327.9 million, DOD's Cooperative Threat Reduction Program is being provided $37 million for projects designed to destroy, dismantle, and improve controls over the former Soviet Union's stockpiles of weapons of mass destruction. DOE is being provided $40 million for its programs in this area.

The provision also calls for the creation of a senior level coordinator to improve the Federal Government's efforts in dealing with the threat of proliferation and to coordinate Federal, State, and local plans and training. Some $2 million is provided for the coordinator to use in focusing research efforts on improved planning, coordination, and training efforts.

Mr. President, the threat of attack on American cities and towns by terrorists, malcontents, or representatives of hostile powers using radiological, chemical, biological, or nuclear weapons is one of the most serious national security threats we face today.

This threat is very different than the threat of nuclear annihilation with which our Nation and the world dealt during the cold war.

During the cold war both we and the Soviet Union recognized that either side could destroy the other within an hour, but only at the price of its own destruction.

I have heard too many experts, whose opinions and credentials I respect, tell me that it is not a question of if but only of when terrorists will use chemical or biological—or even nuclear—weapons in the United States.

In July, the Commission on America's National Interests, cochaired by Andrew Goodpaster, Robert Ellsworth, and Rita Hauser, released a study that concluded that the No. 1 vital U.S. national interest today is to prevent, deter, and reduce the threat of nuclear, biological, and chemical weapons attacks on the United States. The report also identified preventing the loss of control of nuclear weapons and nuclear weapons-usable materials, and the containment of biological and chemical weapons proliferation as one of five cardinal challenges for the next U.S. President.

The Permanent Subcommittee on Investigations of the Governmental Affairs Committee held a series of hearings over the last year on the proliferation of weapons of mass destruction, at which representatives of the intelligence and law enforcement communities, the Defense Department, private industry, State and local governments, academia, and foreign officials described a threat that we cannot ignore, but for which we are virtually totally unprepared.

CIA Director John Deutch, for one, candidly observed "We've been lucky so far."

And, in fact, we have already received at least three loud warning bells. First was the release of deadly sarin gas in the Tokyo subway system. Second was the truck bomb which went off in the garage of the World Trade Center in New York City—a bomb that the trial judge believed the killers intended to be a chemical weapon which, had it deployed as intended, would have killed thousands. Third was the bombing of the Alfred P. Murrah Federal Building in Oklahoma City. The pipe bomb in July in Atlanta serves as yet another warning that we must improve our preparedness for terrorist attacks in this country.

Mr. President, this legislation will significantly improve our ability to deal with this threat—an ability which today is clearly not up to the challenge. We have heard testimony in recent months at hearings held by the Permanent Subcommittee on Investigations that speaks clearly to the remarkable lack of domestic preparedness for an incident involving nuclear, radiological, chemical, or biological materials.

Fire chiefs said that they cannot plan on Federal emergency assistance to help in an emergency of this nature as it is simply too long in coming.

Local emergency first-responders—policemen, firemen, medical technicians—grimly said over and over again that they were incapable of dealing with a chemical or, especially, biological weapon or incident.

By providing funding and a mandate for DOD and DOE to share their experience, expertise, and equipment dealing with nuclear, radiological, chemical, and biological weapons and materials, we can address critical shortfalls in our domestic preparedness that have been specifically and repeatedly noted in congressional testimony and documentation.

Several modest exercises have been held to test how Federal, State, and local emergency responders would deal with a nuclear, radiological, chemical, or biological attack.

In one large exercise, the first 100 or so emergency response personnel—police, firemen, medical personnel—arriving at the scene of a mock chemical weapon disaster rushed headlong into the emergency scene, and were promptly declared "dead" by the referees.

In a second exercise featuring both chemical and biological weapons, contaminated casualties brought to the nearest hospital were handled so carelessly by hospital personnel that, within hours, most of the hospital staff were judged to have been killed or incapacitated by spreading contamination.

In addition, a report recently forwarded by the Secretaries of Defense and Energy to Congress on our preparedness for a nuclear, radiological, chemical, or biological terrorist attack noted that, "response personnel are relatively few in number and pieces of equipment necessary to provide adequate support to an NBC event are in some cases one of a kind."

I still remain fully convinced that the best way to prevent the use of these terrible weapons and materials on American soil is by stopping them before they get here. For this reason, this legislation provides additional resources and impetus for enhancing our ability here at home to detect and interdict nuclear, chemical, and biological weapons and related materials before they get into the hands of terrorists or malcontents.

An extensive study by Arnaud de Borchgrave, Judge William Webster, former Director of the FBI and CIA, Congressman BILL MCCOLLUM, and others, published earlier this year by the respected Center for Strategic & International Studies [CSIS], concluded that "there are few opportunities for detecting, interdicting, and neutralizing these materials once they are beyond the source site. * * * Attention and resources must be directed toward post-theft measures as well."

Mr. President, the single best way to deal with this threat is by preventing proliferation at its source, as far away from the United States as possible. That is why this legislation also bolsters the original concept introduced by Senator LUGAR and myself in 1991, which aims at helping the states of the former Soviet Union to improve their safeguards and controls over existing stockpiles of deadly materials.

The CSIS de Borchgrave-Webster study also found that:

> The most serious national security threat facing the United States, its allies, and its interests is the theft of nuclear weapons or weapons-usable materials from the former Soviet Union. The consequences of such a theft—measured in terms of politics, economics, diplomacy, military response, and public health and safety—would be catastrophic.

de Borchgrave himself stated at a press conference that: "We have concluded that we're faced now with as big

a threat as any we faced during the cold war, when the balance of terror kept the peace for almost half a century."

Finally, Mr. President, this legislation attempts to improve the overall coordination of how we deal with the broad threat to our Nation posed by the proliferation of weapons of mass destruction.

There are currently dozens of government agencies that deal with the various aspects of this threat, with overlapping authorities and programs, but with serious gaps.

Testimony provided in the Permanent Subcommittee on Investigations revealed that coordination between Federal agencies is seriously lacking, and that there is virtually no effective coordination or communication between the Federal Government and State and local agencies and organizations. This appears to be changing, at least in the case of the Olympic games in Atlanta.

I visited Atlanta during the Olympics and received a briefing by a group of representatives from various Federal agencies that were working together to provide security for the Olympic games. I strongly commend their joint efforts, but, this must become the pattern all over the country. We must build from this experience, improve in areas where we have weaknesses, and make this kind of interagency cooperative effort the norm.

Mr. President, I believe this legislation, while only a beginning, responds to a very urgent national security concern of our Nation. I commend all of the Defense authorization conferees for their swift actions in approving the inclusion of the Nunn-Lugar-Domenici Defense Against Weapons of Mass Destruction Act in the conference agreement, and I look forward to the President signing this legislation into law.

Mr. SMITH. Mr. President, I rise in strong support of the conference report on the fiscal year 1997 Defense authorization bill. I want to take this opportunity to commend the distinguished chairman of the Armed Services Committee, Senator THURMOND, for putting together an outstanding bill. Senator THURMOND worked tirelessly to conclude the conference quickly and efficiently, and the product is a bill that we can all be proud of.

I also want to pay tribute to the ranking member, Senator NUNN. Senator NUNN has served on the Armed Services Committee with distinction for 23 years. Throughout that time, he has been steadfast in his support for a strong, capable, and highly prepared military. This will be Senator NUNN's final Defense authorization bill, and I want to take this opportunity to thank Senator NUNN for his outstanding work on behalf of the men and women of our Armed Forces.

Mr. President, the bill before us includes a much-needed increase of $11.2 billion from the President's budget request for national defense. I want to emphasize that even with this increase the total level of Defense spending remains $7.4 billion below last year's level when adjusted for inflation. We are in the 12th straight year of decline in Defense spending.

For the benefit of my colleagues, I want to briefly summarize some of the highlights of this conference bill. The bill before us includes a 3 percent pay raise and a 4.6 percent increase in the basic allowance for quarters for our Armed Forces.

It directs the Secretaries of Defense and Health and Human Services to prepare and implement a demonstration program enabling Medicare-eligible beneficiaries to enroll in the Tricare, the DOD health care program.

The bill approves $10 million in additional research funding to examine the relationship between service of our men and women in the Gulf war and the incidence of congenital birth defects and illnesses among their children.

It also includes $201 million to carry out the Defense Against Weapons of Mass Destruction Act which addresses the Nation's ability to deal with threatened or actual use of nuclear, chemical, or biological weapons against American cities.

The bill provides $40 million to complete development and testing of the Patriot Anti-Cruise Missile Upgrade Program.

It authorizes $32 million for reactive jamming upgrades to the Navy's fleet of EA-6B electronic warfare aircraft.

It includes a $24.5 million increase for night vision goggles and $9.1 million for infra-red aiming lights.

It also directs that the Navy conduct a competitive evaluation of the ATD-111 and Magic Lantern Lidar systems to determine which system to acquire under the Airborne Laser Mine Detection Program.

It provides an increase of $914 million for the Ballistic Missile Defense Organization, and $134 million specifically for the space and missile tracking system.

Last, it approves an increase of roughly $300 million for conventional delivery enhancements for the B-1 and B-2 bombers.

Additionally, Mr. President, I would like to briefly summarize some of the initiatives contained under the acquisition and technology section of this bill. As chairman of the Subcommittee on Acquisition and Technology, I have been troubled by the failure of the administration to adequately invest in long-term technology development. Modernization is the key to long-term readiness, and without effective investment in the technology base, we will be unable to preserve the technological edge that we enjoy today.

The bill before us includes a number of important initiatives to support efforts of the services to develop advanced operational concepts and technologies, to increase the use of commercial technologies for defense applications, and to make defense programs more affordable. For instance, the bill provides $40 million to fund the Marine Corps' Sea Dragon experiments to develop new operational concepts that leverage technology and innovation; authorizes $20 million for a joint services research and development program for nonlethal weapons and technologies; provides $85 million for the dual use applications program; authorizes $61 million for the manufacturing technology programs of the Army, Navy and Air Force; provides an increase of $12 million to continue the procurement technical assistance program; and includes a provision to streamline the Defense Department's requirements for assessing the capabilities of the national defense technology and industrial bases, including cases of unacceptable reliance on foreign sources.

Mr. President, these are but a few of the many critically important initiatives contained in this bill. I would emphasize that these initiatives address the priorities established by the service chiefs and will directly enhance our national security.

I also want to emphasize that each of the issues that President Clinton's advisors indicated may trigger a Presidential veto have been resolved to the satisfaction of the administration. Thus, this bill enjoys strong bipartisan support and the indications are that the President will sign it.

Again, I want to thank the distinguished chairman and ranking member for their outstanding work in formulating a conference bill that enhances national security and reflects the vast majority of the Senate's priorities for defense. They have rendered an invaluable service to the Nation, and I am proud to support this important legislation.

Mr. President, I urge the adoption of the conference report, and I yield the floor.

CHEMICAL WEAPONS DEMILITARIZATION

Mr. MCCONNELL. Mr. President, this morning, I listened to my colleague from Kentucky with great interest as he expressed our mutual concern about the action taken by the conferees on the chemical demilitarization program. I share his disappointment that language which would have guaranteed an alternative technology program so clearly in the interests of our constituents was deleted in conference.

Let me review for a moment how we ended up in this situation and how I hope we can correct course. Several months ago, staff representing all of the Members who have chemical demilitarization facilities met in Senator FORD's office to review the status of demilitarization at each site. At the time, Senator FORD offered a proposal which required the Department of Energy, in conjunction with the Army office which currently manages the incineration program, to develop alternatives to incineration. Although I strongly supported the idea of alternative technologies, the Department of

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 velop reliable threat estimates t will not only help secure governm and military systems, but provide d to the private sector so that they manage their own attendant risks. I otal to this challenge will be foste trust between industry and gov ment in this arena.

Finally, we must be willing to rec sider our previously defined notion national security. The threat fi cyberspace, because it can emar from a borderless world that tr scends national boundaries, elu many of our traditional national s rity assets. We cannot permit problem to get lost in the seams of intelligence, enforcement and defe communities. We will undoubtedly quire the types of international ances that has served us well in our fense of our physical perimeters.

This year the minority staff of Permanent Subcommittee on In tigations completed a lengthy in tigation into these issues that inclu a ... report entitled "*Security Cyberspace.*" The report set forth merous recommendations intended improve our Nation's cyber defen Those recommendations include s key proposals:

(1) Formulate a national policy that motes the security of our information i structure;

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

(3) Complete an intelligence estimat the threats to our information infras ture, that includes an unclassified ver that can be made available to the pri sector;

(4) Promote the creation of an i national computer crime bureau with e gency response capability;

(5) Maintain a better and qualified po computer security professionals and, erally, improve the security consciousne our government's users and managers;

(6) Promote regular computer vu ability assessments, or "red teaming government agencies, especially age outside of the Defense Department; and

(7) Encourage better reporting of com incidents within private industry while ating a mechanism within which ind can report intrusions without fear of inc customer insecurity.

Ultimately, there is no question the information age will bring u new plateaus that will greatly ben our citizens and our world. We r make sure, however, that in our to connect, we do not lose sight of more mundane but equally impor need to protect.•

TERRORISM MEETS PROLIFE TION: THE CONVERGENCE THREATS IN THE POST C WAR ERA

WHEN FICTION BECOMES REALITY

• Mr. NUNN. Mr. President, last ye spoke to a group about the cha that have occurred since the demi