

Mr. SARBANES. It was designed to improve the quality of math and science teachers in the classroom. Now we are being told we are trying to direct where the funds should go. The first point I want to make is that this has a long pedigree coming right from the Eisenhower administration.

Mr. DURBIN. Will the Senator yield?

Mr. SARBANES. Yes, I will yield to the Senator.

Mr. DURBIN. I think it is very interesting. The comments made by the Senator from the State of Washington suggested an enormous percentage of the funds which were being appropriated at the Federal level were spent on administration. I have in my hand an April 1998 report by the Secretary of Education that was requested by appropriators from Congress that is based on data from States, the Coopers & Lybrand financial analysis model, and GAO reports, completed this summer, which I think should be part of the RECORD on this debate, and it says:

One-half of 1 percent of the Federal funding for elementary and secondary education programs is spent on Federal administration.

One-half of 1 percent.

States retain on average an additional 2 percent. The remaining 97.5 percent goes to local school districts.

End of quote from the report. To suggest that it is 50 to 60 percent cost of administration really doesn't square with the facts given us in this report.

Across more than 20 major State formula programs, States, in fiscal year 1995, retained an average of only 4 percent of the money at the State level; they distributed the remaining 96 percent to school districts and other recipients, such as colleges and universities. For the program under the Elementary and Secondary Education Act, the percent retained at the State level was even lower—about 2 percent. For Title I, the largest Federal elementary and secondary program, States retain only about 1 percent of the funds. . . .

The Department uses a very small portion of our appropriation for Federal administration. In fiscal year 1999, we will expend only about \$87 million to administer some \$20 billion in elementary and secondary programs; these funds come from a separate Program Administration budget account, not from funds appropriated for grants to States or school districts. Even with the addition of related research, leadership, and operations costs, the Department spends only the equivalent of about 0.5 percent of elementary and secondary funds for Federal administration.

Mr. SARBANES. I thank the Senator for his intervention. That is a very important point. Because the critics stand up and say it is all going to administration. Now we learn 2.5 percent of it, Federal and State, as I understand it from the Senator, is going to administration. I think we need to underscore that.

I want to come back to this notion that we are trying to direct where the money should go and somehow that is a departure from past practice or hasn't in the past, at least, had strong bipartisan support.

It is clear that math and science is one of the critical areas. I earlier asked

the Senator, wasn't this whole education emphasis important to the U.S. competitive role in the world economy. We can look at what other countries are doing, and we know the kind of investments they are making in math and science. We started with the Eisenhower administration, and that, I think, was at the time of Sputnik that that program was energized to try to improve the quality of math and science. We had some successes, but there has been a relapse, there has been a lapse back, and one of the programs that was cut, as I understand it from the Senator from Massachusetts, and which he is emphasizing we need to restore, is this program to improve the quality of the math and science teachers in the schools all across our country. Is that correct?

Mr. KENNEDY. Yes, absolutely correct.

Mr. SARBANES. Mr. President, it seems to me—and the other program, I take it, is we have a deterioration in the physical quality of many of our public schools in the Nation. Young children are going to school in circumstances that no one would tolerate. In fact, I understand some of these schools do not meet ordinary building standards. And there are serious problems in that regard.

Once again, we are trying to emphasize a program. Of course, another aspect of what the President is pushing for is more teachers in the classrooms so we can have smaller class sizes, which most people agree is extremely important in the lower grades where we are trying to teach reading and we first introduce young people into their education.

In fact, I ask the Senator, what is the situation with respect to overcrowded classrooms across the country?

Mr. KENNEDY. The Senator is quite correct in his general summation of the approach of the President. And that is: One, to have smaller class sizes; two, to upgrade and modernize schools; three, to have an effective after-school program; four, to enhance the quality of teaching in the classroom; five, to ensure that we are going to have access to the new technology and that that is going to be available in the public schools so these children are going to be able to move ahead; six, to raise academic standards for all children; and then seven, to try to get the encouragement to those students to go on to higher education.

That is all part of the partnership, among the local community, the States, and the Federal Government. This is not just a singular effort; this is a partnership. And when you eliminate the Federal assistance in that partnership, you undermine critical support for improving education that is so important to families and their children.

Mr. SARBANES. If I recall the chart that the Senator earlier displayed on juvenile crime, it peaks in the hours I think between about 3 and 8 p.m., which makes the after-school programs extremely important.

Mr. KENNEDY. Yes.

The PRESIDING OFFICER. The time of the Senator from Maryland has expired.

Mr. SARBANES. I thank the Senator.

The PRESIDING OFFICER. The Senator from Kentucky has 15 minutes.

Mr. FORD. I yield the floor, Mr. President, and will take my time later because some here need to go ahead. I am happy to yield.

Mr. KERREY addressed the Chair.

The PRESIDING OFFICER. The Senator from Nebraska has up to 30 minutes under the previous order.

NATIONAL SECURITY AND INFORMATION TECHNOLOGY

Mr. KERREY. Mr. President, in the last 15 years America has been invaded by what has been known as information technology. Like the body snatchers of "Alien" that penetrated deep into the human body, computers and communication technologies have penetrated deep into our lives. Unfortunately, the "Alien" metaphor may not be apt since for the most part we have invited this force into our homes.

We invited these technologies into our homes and our businesses because they allowed us to do things faster, to do things better and to do things cheaper. Among other things these technologies have reduced the cost of running a home, made our businesses more competitive, opened new markets by bringing buyers and sellers closer together, and expanded the horizons of our students not to mention adding entertainment value to our lives.

The good news of computer and associated communication technology have been offset by our growing dependence. To see how much we are dependent one need only look at the high level of concern surrounding the Y2K problem. Computer software is written so that at a second after midnight on January 1, 2000, while hundreds of millions of humans will be celebrating the end of an old millennium and the beginning of a new, our computers will act as if it is January 1, 1900. To the machines this will be the equivalent of day light saving century.

To some this is the beginning of a humorous and good news story: No income tax, a chance to correct the terrible mistakes of the past 100 years, and so forth. However, for those who operate our banking, emergency response, air traffic control, and power systems this will be nothing to laugh at. So dire are the predictions of some who understand how dependent on computers and software we have become that they talk as though they are storing up food and medical supplies just in case.

None of this would have happened if the century had ended 20 years earlier because computers, chips, and microprocessors were not yet running things. Twenty years ago I was hearing people tell me about how computers were

going to change the world. It would be 5 more years before I had my first personal computer: an Apple IIE. In 1983 portable computers were available to those with strong backs or a fork lift. E-mail was in its infancy. The internet was 10 years away from its grand opening to the public. Software was built into mainframes and was available to those who knew how to navigate the procession of prompts and confusing signs. Speed was a snail's pace. Capacity was like a rain drop in the desert.

Mr. President, what happened in the past 20 years is that we were thirsty for the things a computer could do for us. Rapid and accurate calculations enabled even small businesses to get costs under control. Personal computers empowered us. Desk tops enabled us.

Lap tops liberated. Decision making - once driven from the top down by men and women with MBA degrees—has been distributed outward and downward.

Mr. President, now, any PC or Macintosh with average speed and power with state of the art connectivity makes its user a publisher, broadcaster, editor, opinion maker, and analyst of large amounts of previously confusing data.

Advances in computer and telecommunications technology have spurred change and growth in our economy. These changes have generated wealth and jobs by creating new businesses and destroying old ones. Market oriented businesses have had to adjust or perish. Public institutions, because of the nature of democracy—in other words, Majority rules but narrow interests win elections—have been changing much more slowly.

Slowly but surely the work of transferring knowledge from a teacher to a student is being done with the assistance of computers, software, and new systems where new skills are needed.

The vision of this 1998 IRS Restructuring and Reform Act is that this agency will move from a paper to an electronic world. The National Imaging and Mapping Agency—a consolidated combat support agency—will in a few years talk about maps as those things we used in the good old days back when dinosaurs roamed the Earth.

In fact, nowhere are the changes of the computer age more pronounced than in our military and intelligence gathering forces, which is what I choose to discuss on the floor today. Computers and communication technologies have made America's fighting forces stronger and more effective. We should be proud of the men and women who have trained and prepared themselves to take advantage of these new tools.

However, we also need to be alert to a hard truth: With strength comes vulnerabilities. Just as Achilles was held by his heel as he was dipped in the potion that made him unbeatable, we need to be alert to those small spaces where a determined enemy could do us great harm.

If we are to maintain our economic success and provide the security our citizens expect and deserve, we must as a nation turn to address our weaknesses.

The ability of people to use information technology to reach into our homes and to amass vast amounts of personal data threatens our sense of privacy. The omnipresence of this technology has caused our society to develop a dependency on silicon chips and the wires that connect them. And, the connectivity that now brings us so many benefits may also be a vulnerability that nations and terrorists could use to threaten our security.

We have been blessed by our dominance in high-technology industries and in our society's acceptance of new information technology. Information systems are the backbone of America's telecommunications and electrical power grids, banking and finance systems, our transportation systems, broadcast and cable industries, and many other businesses besides. They have helped American workers become more productive, have brought new efficiencies in the use and distribution of resources, and have helped our Nation grow to be the most advanced and competitive economy in the world.

We owe a large part of that success to the ingenuity, perseverance, and vision of America's information technology companies and their employees. The story of how computer companies started in garages can grow into multi-billion dollar corporations is almost legendary. An industry virtually nonexistent twenty five years ago has brought enormous wealth and opportunity to thousands of Americans.

Mr. President, information technology has transformed our Nation's economy, and, as we enter into the 21st century, our Nation's livelihood will depend on continued development of this industry. But the wonder of this technology is how its success has brought extraordinary changes to other aspects of our lives.

Modern information technologies provide us with unheard-of opportunities in education, business, health care, and other life-enriching areas. Information technology empowers people to continue their educations and upgrade their skills throughout life. Education no longer ends at the schoolhouse door. In addition, new technologies are extending lifesaving medical care to remote rural areas and promoting healthy communities across the country. These new avenues to information better inform our electorate, and the improved means of communication make it far easier for individual citizens to express their views to the general public and to their elected representatives.

In combination, these technological benefits allow people—both young and old—to develop new skills, explore new interests, and improve their lives.

America's technological strength is the envy of nations around the globe.

But that strength, if not understood and protected, may also be our Achilles' heel.

We have been blessed this year with a number of warnings about this grave and far-reaching threat. We have been blessed with warnings about the interdependence of our information infrastructures, the interlocking network that can make local hospitals and airports victims just as easily as multinational corporations and media conglomerates. We need to heed the warning and respond to this danger.

Just a few weeks ago, the media reported that the electronic mail programs the vast majority of Americans use had vital, hidden flaws.

Simply opening an e-mail message could unleash a malicious virus and allow that virus to freeze your computer, steal data, or erase your hard drive. I realize there are some people in the United States—many of them here in the Senate—who still do not use e-mail. But our society today relies upon electronic mail for use in Government and commercial communications, for business management and project coordination, and personal entertainment and missives. A malicious person could potentially have used these flaws to blackmail people or companies, to disrupt Government and commercial activity, or to sabotage civilian or military databases.

Just a few months ago, one satellite orbiting more than 22,000 miles above the state of Kansas began tumbling out of control. It was the worst outage in the history of satellites. By conservative estimates, more than 35 million people lost the use of their pagers, including everyone from school children and repairmen to doctors, nurses, and other emergency personnel.

All of that was the result of one small computer on a satellite 22,000 miles into outer space.

Earlier this year, we were in the middle of a very tense standoff with Saddam Hussein. And we were able to track an attack on the Pentagon's computer system to a site in the Middle East, in the United Arab Emirates. There was a legitimate question at the time: Was this an act of war? Was it a terrorist? Or was it, as it turned out to be, teenage hackers inappropriately and illegally using their home computers? The implications of an effective attack against our military's information systems would be devastating during a time of crisis. This attack failed, but will we be as fortunate in the future?

I do not think these incidents are a statement about software companies, the satellite industry, or teenage computer aficionados.

These incidents are a warning—loud, clear, and wide—about the dependence of the American economy and the American people on information technology. Our use of information technology has helped us achieve and maintain our status as the world's strongest

nation. But our dependence on information technology also brings exploitable weaknesses that, like the Lilliputians to the giant Gulliver, may enable our weaker adversaries to cause great damage to our nation.

In Jonathan Swift's tale, the Lilliputians used their mastery of mathematics and technology to defeat their much more powerful adversary Gulliver. Today, weaker adversaries may use their mastery of information technology to invade our privacy, steal from our companies, and threaten our security.

The revolution in Information Technology has propelled the United States to an unparalleled position in the global economy. The principles of freedom and democracy that we champion are ascendant throughout the world.

We have the world's largest economy, and we trade more than any other nation. Our military strength, in conventional and nuclear terms, is greater than that of any other nation. In short, we are the sole remaining superpower in the world.

And yet, we still find ourselves vulnerable to individuals or groups—terrorists, criminals, saboteurs—who have a fraction of the manpower, weaponry, or resources we possess. In many ways, we are a technological Gulliver. America's massive shift toward an economy that is based on information technology has been a mixed blessing. Because we have the most complex, multifaceted economy, we are a multifaceted target.

And our strategic vulnerability has risen hand-in-hand with our economic power. Like the Lilliputians, there are people who have used the principles of mathematics and science to master technology.

They are so small in scale compared to the threats that we usually see that we have to strain our eyes just to identify them and figure out what they are doing. Gulliver, if you recall, did not win his freedom with a single act or weapon. He used a combination of things: sometimes he used his power, sometimes he used wit, and he learned from his experience how to deal with his adversaries.

Mr. President, Congress urgently needs to establish a bipartisan agenda designed to create more economic opportunities in technology and to close our vulnerabilities. The following is my attempt to suggest what is needed:

1. We need more competition, not less. Congress passed the Telecommunications Act of 1996 with the hopes of increasing competition and improving access to communications technologies. Unfortunately, competition has not developed on the scale anticipated when the Act was passed.

Nearly 3 years after the Act, most telecommunications customers lack the ability to simply switch telephone companies. In 1999 I hope Congress will make changes in the law needed to bring the benefits of competition—lower prices and higher quality—to the American household.

2. We need a special effort to make technology a part of our educational system. More money should be appropriate for research and training. Regulations need to be written so the market can offer curricula-relevant courses to students in the home and school. We need to settle the disputes surrounding the E-Rate so our school boards can plan and budget accordingly.

3. We need bipartisan agreement on how to protect privacy and security. The encryption debate has hobbled our efforts to write laws that enable our law enforcement and national security agencies to carry out their mission of keeping Americans safe while harnessing the power of the market to increase security and privacy.

Any discussion of security on-line must inevitably involve encryption issues. Over the past five years, the debate over encryption policy has pitted law enforcement, national security, privacy, and commercial interests against one another. Yet, all these interests would agree that providing security in our public networks is essential to fully exploit the potential of information technology.

Personal privacy in the digital world should not suffer at the hand of unreasonable export laws. Therefore, Congress should take action in the coming year to remove export restrictions on encryption products of any strength. I am confident that through cooperation between Government and industry, encryption can be exported without compromising the legitimate needs of law enforcement and national security. A compromise can be crafted if all parties, both private and public, are willing to work together to solve the common goal of maintaining America's national security in the new digital age.

4. We should create in law a panel consisting of members of Congress, Administration officials, and leaders in high-technology industries to address the implications of information technology on our society and our security. We should also create a new national laboratory for information technology that will both perform research in this field and serve as a forum for further discussions of the issues arising from information technology.

Mr. President, it is this fourth idea—a new panel and a new laboratory—that I would like to discuss today. Why do we need this?

We need this, for starters, because the new threat of information warfare requires a new paradigm in which the military must rely like never before on other organizations and institutions to achieve success.

Even if all of the information safeguards for the Defense Department's data, equipment, and operations were airtight, that would not be adequate. Currently, more than 95% of all wide-area defense telecommunications travel on commercial circuits and networks. And it would be impossible to replicate that type of capability on our own.

Should an electronic attack come, it will likely not be aimed just at military targets, but at civilian sectors as well. It is not simply that the private sector relies on the military. The military relies on the private sector.

That is one reason we as a government cannot afford to ignore the defense of the public and private sector infrastructure: We cannot do our most basic job—protecting national security—without that.

In this new world of technology, if one of us gets tripped, we all risk a fall.

Our Government, as it is now organized, can scarcely cope with these new challenges. We need to address the development and vulnerability of the American information infrastructure now. The regulatory frameworks established over the past 60 years for telecommunication, radio and television may not, in fact, most likely will not, fit the Information Economy. Existing laws and regulations should be reviewed and revised or eliminated to reflect the needs of the new electronic age.

As a government, we need to reassess the areas of responsibility of our different parts, and the lines of authority that connect them, to ensure we are best organized to face this threat.

More than two dozen federal agencies have either jurisdiction or a direct interest in the regulation of information technology as it applies to national security or electronic commerce. The Congress is no better off. In Congress, some 19 committees are responsible for legislation on the same issues.

The Government has much to offer, through our understanding of security concepts and technology, along with the vulnerabilities of information technology and systems. We are strongly committed to share this knowledge with the private sector. Such partnerships are crucial, but there are some pitfalls, and we will need to build a balanced approach. For example: We have to be careful not to give the impression that Government wants to increase its involvement in the day-to-day operations of individual businesses.

This is not at all the case, and few things will drive the private sector away like the potential for more Government intrusion and regulation.

“Government Knows Best” is not the message we want to send.

As a general principle, Government should step in only when problems exceed the capabilities of the private sector and the remedies of the marketplace. However, in cases where there are no reasonable business reasons for companies to make preparations, such as to counter a coordinated, simultaneous attack against multiple infrastructures, then Government should be prepared to provide economic incentives and support.

A natural market exists for security and, ultimately, that will be our best course of action: a solution that combines the entrepreneurial strength and energy of the private sector with the national mission of the Government.

One cannot overstate how important it is to get the Government-industry relationships right, because without them as a foundation, the value of all other efforts will be significantly diminished. A fundamental challenge in many cases is getting information about vulnerabilities and threats itself, and this simply cannot be done without the foundation of public-private sector information sharing. We cannot solve this by unilateral Government efforts. We have to move together to solve it.

Mr. President, it is no surprise that both the Government and private sector are finding this difficult and complicated and frustrating. To combat cyber attacks—whether by terrorists, spies, disgruntled employees, pranksters—one needs both technical sophistication and cooperation among numerous companies, agencies and nations.

It is going to be imperative for the protection of our information infrastructure that the private sector, national security officials, and law enforcement work together—not just on this issue, but on issues for the future.

Many fear these discussions would lead to Government intrusiveness and abuse of power. Americans have always had a healthy skepticism towards Government power and our Constitution sets strict limits on what Government can and cannot do. We are a strong and vibrant nation directly because we enjoy rights of free speech, free assembly, and against unreasonable searches and seizures. Information technology can allow us greater exercise of those rights. When we examine the security of information technology, these rights must remain our guiding principles, and our Government policies should reflect them.

We must get past the suspicion between the private sector and Government and move forward. The information infrastructure is vital to America's defense and to America's economy and we cannot preserve one without protecting the other.

Here we need two things: First, we need a mechanism that transcends narrow organizational politics to bring consensus; and, secondly, we need a facility for advanced research into information technology protection that also provides a venue for constructive and ongoing dialog with industry, the Government, and academia.

I believe Congress should act as soon as possible to create a blue-ribbon panel of top federal officials, key leaders from Capitol Hill, and experts from the high-technology field to address the issues of information assurance, infrastructure protection, and encryption that cut across committee lines. We need to have a panel that can speak with authority on both politics and policy.

From the White House, we need to see a commitment of time, attention, and resources at the highest levels.

Cabinet officers need to play an active role in shaping the solutions that

are going to emerge from such a panel. These issues are complicated and they have far-reaching implications, so at the end of the day we need to have leaders in their respective areas—Cabinet and Cabinet-level officials—who are prepared to forge the necessary compromises and make the case to industry and to the public. Congress needs to take a similarly pragmatic approach. Committee chairpersons, with their expertise in different areas and institutional memory, need to be on this panel and give it all the attention they would a piece of legislation. But in addition we need to acknowledge the politically charged nature of these issues and be prepared to deal with them. So I propose that we not only have representatives by issue area, but representatives who are designated to speak for each major faction in the Congress: a representative of the majority in the Senate, and one for the House, a representative of the minority in the Senate, and one for the House, and representatives of the legislative caucuses that have an interest.

Clearly Government cannot do this alone. We need the perspective, the insight, and the vision of experts who are part of the developments in the information technology field and who can predict on the basis of that experience where technology is going. We need their expertise and a willingness to work with their government, for otherwise this problem will only grow worse. The panel I envision must therefore have a strong component of private sector experts devoted both to the advancement of technology and to the security of our country.

The complement to this Congressional panel should be a forum where Government, industry, and academic officials can work on these problems in a systematic, confidential, and dispassionate way. I propose that we learn from our experience and look to those models of industry-and-Government cooperation that have worked in the past.

We can learn from agencies like the National Safety Transportation Board, DARPA, and other federally funded research and development centers. Specifically, Congress should pass legislation that would enable the President to create a new national laboratory and research facility to address information infrastructure protection. The role and mission of such an organization would be to target those specific areas that are now suffering from sporadic, contradictory, or insufficient attention.

We must have a structure that can address the entire range of national security planning and execution—in other words, threat assessment and evaluation, development of requirements, R&D, acquisition and procurement, development of strategy and the conduct of operations across the entire spectrum, from large-scale conflict to peacekeeping and operations other than war. But this center would also

help develop techniques, policies, and procedures to make civilian and commercial information technologies secure.

To accomplish that mission, the information technology laboratory would have to: Support research and development by industry or Government-industry consortiums that aims to protect our privacy, shield our commercial interests, and defend our nation against information technology threats; ensure that there is a secure conduit for the exchange of information about security threats; provide a forum for developing and managing responses and contingency plans, both directly and in cooperation with a national command authority.

The Information Technology Laboratory would be funded through annual appropriations as a Federally Funded Research and Development Center. But it should also be able to establish fee-based contracts with agencies of federal, state, and local government as well as universities for specific services so that budget costs could be kept to a minimum.

The Information Technology Laboratory could also contract with private industry to do research and development, while taking special precautions to protect the confidentiality of proprietary data or information. The laboratory would also report annually to the appropriate oversight committees in Congress and the President.

In just four years from now, knowledge and information workers will make up one third of all the workers in our multi-trillion dollar economy. We can create a safe corridor for their passage to the next century. Or we can continue to talk past each other while the Information Superhighway attracts more and more robbers and frauds and terrorists.

We need to come to this task with a clear sense of purpose and full understanding of the urgency involved. America has gained much from information technology, and stands to gain much more as these systems mature. Our future depends on the success of this technology.

But that success and our security depend on finding the policies and practices that will identify and correct vulnerabilities before they are exploited. Together, I am certain we can address this problem. In a noble but imperfect democracy such as ours, answers are not impossible, they are only impending. I look forward to working with my colleagues to face this challenge. I yield the floor.

Mr. CRAIG addressed the Chair.

The PRESIDING OFFICER. The Senator from Idaho is recognized.

UNANIMOUS-CONSENT AGREE-
MENT—CONTINUING GOVERN-
MENT FUNDING

Mr. CRAIG. Mr. President, on behalf of the majority leader, I have a couple of unanimous-consent requests.