HEINONLINE

Citation: 4 Bernard D. Reams Jr. Law of E-SIGN A Legislative
of the Electronic Signatures in Global and National
Act Public Law No. 106-229 2000 H974 2002

Content downloaded/printed from
HeinOnline (http://heinonline.org)
Sun Apr 21 22:02:48 2013

-- Your use of this HeinOnline PDF indicates your acceptance
of HeinOnline's Terms and Conditions of the license
agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from
uncorrected OCR text.

think a bit of legislative history is interesting here.

Mr. Speaker, first business groups complained that without these provisions they would not be able to advocate for an employee not being treated fairly by their HMO. So the gentleman from Georgia (Mr. NORWOOD) and I put those exceptions into the bill. Then those same business groups complained that the exceptions were in the bill. You just cannot please some people.

Now let us talk about the punitive damages protections in the House bill. This is another case in point of how you just cannot please some people. This provision was suggested to me, as a matter of fairness, by members of the industry. They said if we are going to be bound by the external review board's decision and if we follow the board's decision, then we should not be liable for punitive damages, quote/unquote.

Know what? I agreed, and this provision in my original bill was incorporated into the Norwood-Dingell-Ganske bill. Maybe Heritage does not think that this provision is significant, but that is not what I have heard from the industry. Remember, this punitive damages relief would apply to all health plans under our bill, not just to group health plans.

While the Heritage paper closes by saying that the bipartisan House bill would result in, quote, a staggering amount of red tape for American doctors and patients, unquote, well, Mr. Speaker over 300 patient and professional organizations have endorsed the bipartisan House bill. Spare them your crocodile tears, please.

The Heritage paper also quotes Professor Alain Enthoven, a health policy analyst, from his paper, "Managed Care: What Went Wrong? Can It Be Fixed?"

Mr. Speaker, the Bipartisan Consensus Managed Care Improvement Act will go a long way to fixing the problem that Dr. Paul Ellwood, the father of managed care, expounded on at a Harvard conference last year. In speaking of the takeover of health care by managed care, Dr. Ellwood said, quote, "Market forces will never work to improve health care quality, nor will voluntary efforts by doctors and health plans. It does not make any difference how powerful you are or how much you know, patients can get atrocious care and can do very little about it."

Remember, this is the originator of the concept of managed care. He goes on to say, "I have increasingly felt that we have to shift the power to the patients. I am mad," he said, "in part because I have learned that terrible care can happen to anyone."

Mr. Speaker, the Norwood-Dingell-Ganske bipartisan House bill which passed this House with 275 bipartisan votes would shift that power to the patient. I sincerely hope that the conference committee gets the message.

CYBER TERRORISM, A REAL THREAT TO SOCIETY

The SPEAKER pro tempore. Under the Speaker's announced policy of January 6, 1999, the gentleman from New Jersey (Mr. ANDREWS) is recognized for half the remaining time until midnight, approximately 50 minutes, as the designee of the minority leader.

Mr. ANDREWS. Mr. Speaker, I want to begin by expressing my appreciation to the Chair at this very late hour and to the members of the staff who are so diligently working here with us and for us at this very late hour as well.

We are gathered tonight at a time of unprecedented peace and power for our country. Because of the enormous dedication and sacrifice of Americans who have served in our armed forces throughout history, around the world in the past and at present, our country is stronger and more secure than it has ever been, and that is a blessing for which we are truly thankful.

Certainly that thanks is directed at those who wear the uniform of our country tonight around the world and those who have so nobly worn it in the past. It is truly a gift and a legacy that we enjoy tonight.

Our relative strength in the world does not mean that we live in a purely safe world, a world without risk. We must endeavor not to repeat the mistakes of history, where very often at times when we felt most safe we were most vulnerable.

There are clearly three areas of major threats to our country's security as we gather tonight. The first is the threat of an emerging competing global superpower in the People's Republic of China. The second is the continued virulent presence of regional negative hostile dictatorial forces such as Saddam Hussein in the Persian Gulf, President Milosevic in the former Yugoslavia. Those two threats, the threat of China and the threat of those regional dictators, are very severe threats indeed. I trust that in the coming weeks and months we will consider as a Congress, along with the executive branch and the military, ways to confront those threats.

This evening I want to spend, Mr. Speaker, some time talking about a threat that is not so easily detected, is not so obvious, but a threat that I believe is truly lethal and deadly, a threat that is unlike any threat that we have faced in the history of our republic, and that is the silent but deadly threat of cyber terrorism, the quiet but lethal assault on our country's systems and people, which I believe will be one of the major issues in the new century, the new millennium, in the defense of our country.

Unlike the growth of a large superpower army, unlike the proliferation of arms from a hostile nation state, we cannot readily or easily see the development of the cyber threat. I pray that we may never feel it and tonight I would like to talk about how we can prepare for it.

I would like to begin by talking about what has already happened to make it clear that our subject tonight is not an imaginary one. It is all too real. Listen to George Tenet, the director of the Central Intelligence Agency, speaking a few months ago. He said, and I am quoting, "An adversary capable of implanting the right virus or accessing the right terminal can cause massive damage to the United States of America," the right virus or the right terminal.

□ 2215

In 1998, two youngsters in California, directed by a hacker in the Middle East who was later described as the Analyzer, launched attacks which disrupted our troop movements in the Persian Gulf. These two young hackers, based in California and directed by the Analyzer in the Middle East, disrupted troop deployments to the Persian Gulf in February of 1998 from California, launched attacks against the Pentagon systems, the National Security Agency and a nuclear weapons research lab.

The deployment disruptions, that is, the disruptions in the deployment of our troops around the world and the Persian Gulf, from a computer terminal in California, were described by Deputy Secretary of Defense John Hamre, a real leader in this field, as "the most organized and systematic attack" on U.S. defense systems ever detected. In fact, they were so expertly conducted that President Clinton was warned in the early phases that Iraq was most probably the electronic attacker.

Two teenagers steered and directed by a master hacker halfway around the world, launching what our number one defender has called the most organized and systematic attack on sophisticated defense computer systems, so sophisticated that in the early hours of the attack the President of the United States was told by his most wise and knowledgeable advisers that Iraq was the electronic attacker. It was not Iraq, it was two U.S. citizens directed by a hacker in the Middle East.

On March 10, 1997, another teenager, this one based in Massachusetts, invaded a computer system run by the Bell Atlantic company in Massachusetts, knocked out telephone communications, among them telecommunications, telephone service, for the Worcester, Massachusetts air traffic control system at that airport in western Massachusetts. The tower was knocked out for 6 hours.

Let me read from a report from the Boston Globe of March 19, 1998. "The computer breach knocked out phone and radio transmission to the control tower at the Worcester airport for 6 hours, forcing controllers to rely on one cellular phone and battery powered radios to direct planes."

One teenager hacking into a computer system of a major regional telephone company, knocking out for 6

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H974 2002

hours the telecommunications capacity of an entire area, and including an airport. And as people flew through the skies above Worcester, Massachusetts, the air traffic controllers relied on one cell phone and battery powered radios to direct the planes.

Joseph Hogan, who manages the control tower at Worcester and 26 other airports for the Federal Aviation Administration, said this: "We relied on our back-up systems, and, thank goodness, they worked. Had we been busier, the potential for a serious incident with dire consequences was there." Six hours.

In 1997, our intelligence community conducted what was called Operation Eligible Receiver, a war game played in cyberspace, an intelligent and far-reaching attempt by the U.S. military and intelligence community to game out what would happen if a hostile foreign power tried to attack our systems around the country.

A so-called red team put together by the intelligence community pretended to be North Korea. Thirty-five men and women specialists, 35 people using hacking tools freely available on 1,900 web sites, Mr. Speaker, any of our listeners tonight could access on their home computer right now. These 35 men and women accessing those 1,900 web sites in the public domain managed to shut down large segments of America's power grid and silence the command and control system of the Pacific Command in Honolulu.

The Defense Information Systems Agency, DISA, launched some 38,000 attacks against its own systems to test their vulnerabilities. Only 4 percent of the people in charge of those targeted systems realized they were under attack, and, of those, only 1 in 150 reported the intrusion to the superior authority.

We had a war game, and the good guys lost. The smartest and most capable people that we have were rather easily outwitted by this war game.

A Pentagon report goes on to say that probing attacks against the Pentagon, there are tens of thousands of them a year, are routed and looped through half a dozen other countries to camouflage where the attack originated. Information warfare specialists at the Pentagon estimate that a properly prepared and well-coordinated attack by fewer than 30, 30 computer virtuosos, strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees. Such a strategic attack mounted by a cyber-terrorist group, either sub-state or non-state actors, that is to say either terrorist groups that are not part of any state or terrorist groups that are sponsored by a rogue state, would shut down everything from electric power grids to air traffic control centers. A combination of cyber-weapons, poison gas and even nuclear devices could produce a global Waterloo for the United States.

In 1999, the Pentagon tracked 22,144 intrusions on its own sensitive computer systems. 22,144 times in the last calendar year people figured out how to hack their way in to our most vulnerable systems. That is according to Major General John H. Campbell of the United States Air Force.

Deputy Secretary Hamre reports that his sources show that there are at least 20 countries who presently have information warfare strategies and operations active against the United States. This is an overwhelming and compelling body of evidence that says that this is not a question of whether we will be prepared for something that will happen to us in the future; this is a question of how well we are prepared for something that is happening to us right now, tonight, around the world.

Now, there is good news to report. As a member of the Committee on Armed Services, I have had the opportunity to meet and listen to and be briefed by some incredibly committed and talented men and women, both in the civilian service of this country and the Department of Defense and in the uniform of this country in the branches of our armed Services, and also serving in the various intelligence agencies of this government.

Mr. Speaker, we are blessed tonight with a robust, dynamic and bright corps of young men and women who are committed to defending their country. With the tools that we have given them, they are doing a magnificent job. Deputy Secretary of Defense Hamre is the leader of this effort and deserves special praise. His Assistant Secretary, Art Money, deserves special praise, and so do many others who work at their direction who have foreseen this problem, have been so diligent in pursuing it, and are truly inspiring in their level of preparation.

I have no doubt, no doubt whatsoever, that if we do our job, Mr. Speaker, and give these civilians and uniformed personnel and intelligence personnel the tools to do their job, they will excel in doing their job and protect our country.

This issue is not new to this floor. The gentleman from Pennsylvania (Mr. WELDON), my friend and colleague from nearby Pennsylvania, has been working on this issue years before it found its way into the headlines. He is serving as the Chairman of the Subcommittee on Research and Development of our Committee on Armed Services and has been a long time advocate of this cause.

The gentleman from South Carolina (Mr. SPENCE), the chairman of the Committee on Armed Services, a Republican, and the gentleman from Missouri (Mr. SKELTON), the Democratic ranking member of the committee, have very wisely appointed a special task force of our committee to focus on cyber-terrorism in this year's defense budget. That special committee is ably chaired by my neighbor and friend, the gentleman from New Jersey (Mr. SAXTON). The members of the committee are truly dedicated to this purpose, and I believe that the efforts of Chairman SPENCE and Mr. SKELTON and Chairman WELDON and Chairman SAXTON and those of us working with them on this effort are going to elevate this issue in this Congress, in this defense budget and defense bill, and take some important steps that really need to be taken.

Now, these steps would follow on the heels of the President's directive number 63 which was issued on May 22, 1998. That directive, which is well under way, is a good first step toward addressing the very real problems that I talked about tonight. But I think we have to build on those steps and understand the very unique nature of the problem before us.

Our country is organized, and well organized, for the world of physical space. Our military strategy has always been about protecting and defending key points of territory, the seas, land, so we could protect the sovereignty and rights of our people. We have always recognized a distinction in our civil law between civilian and military, between police action and law enforcement on the one hand and military action on the other.

These are time-honored and wise distinctions that we should never forfeit, but they are distinctions based on the physical world. And when we deal with the world of cyber-terrorism, we need to rethink them. By no means should we abandon cherished principles that recognize that civilian authority rules our country and the military serves civilian authority. By no means should we abandon the principle that recognizes the rights of Americans to enjoy privacy in their homes, the reasonable expectation of privacy in their affairs.

By no means should we forfeit those principles, but by no means should we permit those who would do us harm and terror to hide behind those principles to abuse the purposes of those principles and subject the country to horrible acts of destruction.

This month I will be introducing legislation that creates a strategy to address what I believe are the three great questions posed for our country by the here and instant onslaught of cyber-terrorism.

The first question is how can we make sure that our military is fully prepared? The President has given us great guidance in this in his budget proposals for the new fiscal year. He has set aside $91 million, not for software or fancy computers or bricks and mortar, but he set aside $91 million so we can be sure that the smartest and most motivated Americans serve their country in this field. Scholarships for bright young students, continuing education for those who already serve, institutes and centers and programs for people to come together from the worlds of business and academia and government and the military and think about ways that we can address and solve these problems.

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H975 2002

I believe, based upon the classified briefings I have been privileged to receive and the record in the public domain, that the U.S. military, the U.S. intelligence community and the civilian employees of the Department of Defense are ahead of the curve in this area. We are by no means invulnerable in our defense infrastructure, but this is a problem that has been thoroughly analyzed, and I believe we are well on the way to thoroughly protecting the key defense infrastructure of our country in military bases around our country and around the world.

But that leads us to the second question, which I am not so confident has been resolved, and that is what can we do to protect ourselves against the place at which we are most vulnerable, and that is in the civilian infrastructure and civilian systems of our country?

□ 2230

When the California hackers hacked into the Pentagon computers and disrupted our troop deployments in the Persian Gulf, it was shocking. But the Defense Department has acted swiftly and, I believe, powerfully, to prevent future repeats of this problem, future manifestations of this problem.

The same really cannot be said of our civilian sector, of the air traffic control system, of water and power utilities, of our banking and financial system, of our transportation and law enforcement systems. Not because these people are not doing their jobs; they are doing a very good job, Mr. Speaker. But I think the same level of confidence cannot be stated about civilian institutions because they are civilian institutions. Thank God for the fact that the United States of America is not organized as a military society.

In our country, the military does not run the airports, the military does not run our court system or our 911 system or our water and sewer and power systems; and may they never, because we are not that kind of society and the military is not designed for that purpose in America. These systems are run by some combination of public and private institutions that do a wonderful job of fueling and supporting the strongest economy in the world, but they are not organized for the purpose of preventing cyber-terrorism.

The phone companies are organized for the purpose of making our calls go through and our data. The water and sewer and power utilities are organized for the purpose of making the lights go on when we turn the switch and the water go on when we turn the faucet and the heat go on when we turn the thermostat up. The air traffic control system is designed to get us safely from one point to another. The 911 system is designed to dispatch the brave and courageous men and women who ride in our police cars and who drive our ambulances and serve on our fire trucks and other emergency vehicles. Those systems work.

Late in 1999, we saw as a country that we had a major and comprehensive effort to make sure that accidental breakdowns in that system would not paralyze and cripple our country. The phrase "Y2K" became forever embedded in our national lexicon, and it was an American success story. At my house, we filled our bathtub up with water on New Year's Eve and made sure we had all the flashlights ready and made sure we had some means of communicating with our loved ones, because we were not sure, were not exactly sure that the water would work or the lights would stay on and the phones would work the next day, or at 12:01. To the everlasting credit of America's institutions, in most cases, in most ways, everything worked, because we were prepared.

But the Y2K story was really just the tip of the iceberg, Mr. Speaker, because the real question is what if somebody intended to do us harm. What if it was not an accident that the computer systems turned over from 99 to 00, but what if someone who could not defeat us by dropping bombs on our power plants or could not defeat us by having an army invade our shores decided to defeat us and create chaos in America by hacking into our systems on purpose and create that kind of havoc? Are we prepared? I think the answer is not nearly well enough, as the incident in Massachusetts in 1997 shows.

So what do we do about it? Well, there are three approaches we could take and two of them are absolutely wrong. One approach would be to say that let us militarize everything, let us be sure we can defend our airports and our power plants and our phone systems and our 911 system; let us put the military in charge of it. There is no one, I trust, in this House and no one, I am certain, in America's military establishment who would want that result, nor would I.

The second approach would be to say, let us just see what happens. Let us let the normal market forces which work so well in organizing our economy handle this problem. I know of very few captains of industry who would be so naive as to agree with that statement. Our phone companies, our power companies, our transportation companies are not organized to defend against terrorists, nor should they be. They are organized to deliver goods and services at a profit or in the proper way to the public.

So there needs to be a third approach that is a partnership between and among the military community, the intelligence community, the private sector, the academic sector, and law enforcement. I think that American ingenuity in the utility companies and the telecommunications companies, in law enforcement could absolutely do this job and make us thoroughly well prepared for the cyber-attacks which are happening to us as we speak, but they need help. My legislation will propose that very high standards be set, the same way they were for Y2K. They will propose an active, cooperative system between and among our military and our law enforcement and our civilian entities, and it will propose reasonable and well-targeted financial assistance for those aspects of industry and the private and civilian sector that reach the goal most expeditiously and most efficiently.

There are precedents for this, Mr. Speaker. Our MIRAD program, our shipbuilding program is a good precedent and it works this way, and my legislation will reflect this principle. We say to certain shipbuilders that if you are building a cargo ship, the Government of the United States will subsidize in part the construction of that ship through loan guarantees and direct contributions. We will help you build your ship. What you need to do for us in exchange is to make that ship available at a time of national emergency, to carry military cargo so we can deploy our troops around the world if and when necessary. It is burden-sharing between the vibrant commercial sector and the military and law enforcement carrying out its mission to defend and protect the country.

That is the approach that I think we should take in our bill, is to share the burden with the dynamic private sector, but encourage and indeed require that sector to bring its level of protection up so that when someone wants to hack into an air traffic control system, when someone wants to mask the computers at the water utility so that when the person reading the water utility computer screen thinks there is no arsenic in the water because that is what the printout says, but there is arsenic in the water because someone has bugged the computer, there is a backup system. Or when someone, and this has happened, hacks into the telephone system and reroutes 911 calls to a pornographic call-in line, as has happened, or a pizza delivery service, as has happened, chaos will not occur; but there will be a backup system in place.

The third thing that my legislation will do is to answer the question of prevention, and prevention is what we most want. We want our military to be able to protect us so that we can prevent cyber-attacks. We want our civilian sector to ramp up its efforts so that we can be protected from cyber-attacks. However, sometimes they are still going to happen, as they did in 1998 when the California hackers, aided by the Middle East hacker, disrupted our troop deployment; as it did in 1997 when the airport air traffic control system in Massachusetts shut down for 6 hours. It is still going to happen.

How do we very quickly find the perpetrators and understand whether this is a law enforcement problem that requires prosecution in our criminal law enforcement system or whether it is an international terror problem that requires a military or diplomatic response.

There are two changes that I believe are foremost of importance that will be

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H976 2002

in the legislation that I propose. The first change is a change that says to the Department of Defense, we are going to take the handcuffs off of your hands and when a Defense Department information system or computer is attacked, we are going to let you find out who did it.

I think most Americans would be amazed, Mr. Speaker, to find out that we have a law that works this way: if tonight a hacker hacked into an important Defense Department software system or computer that affected the launch codes for our nuclear weapons, or that affected our defenses against poison or nerve gas, we have a law that says, until the law enforcement people conclude and prove that the hackers are foreign agents, the Department of Defense cannot do anything about it. They have to wait until the law enforcement people conclude that it is not a domestic threat, it is foreign. In other words, we treat these hackers the same way we would someone who is running an illegal NCAA basketball betting pool on-line.

Now, I do not for one minute disregard or impugn the abilities of our law enforcement people. They do a great job. But their job is to deal with organized crime or with those who would do harm within America. It is certainly not to deal with the Libyan special services forces or with people in North Korea who would do us harm.

We need a law which says, when the Department of Defense's computer systems are under attack, they do not have to wait to find out who did it, that they can immediately and expeditiously figure it out and take whatever steps are necessary, consistent with our Constitution and consistent with our law to do something about that.

The second change that I think is imperative is that we change the law so that our government can find out more easily about criminal records of people in very sensitive jobs that affect government infrastructure. Believe it or not, right now, if the following occurred, the Department of Defense and others would have a hard time getting information. Let me sketch this scenario.

If what happened in Massachusetts in 1997 had happened because a vendor who was working for the phone company as a troubleshooter deliberately sabotaged the air traffic control system, and that vendor had someone working there who was a spy for the vendor; and that spy, in fact, had some kind of criminal record at the State or local level that would attach that spy's conduct or relationships with foreign agents, and we had in our CIA database evidence that if we knew that this spy, if we knew about his record that we could figure out who was hooked in internationally, our military people cannot get access to the State and local criminal records of that spy. It is illegal. It is unbelievable.

The fourth amendment does not give someone who wants to do harm to the people of this country license to do so with impunity. There is no Member of this body who is more committed to the principles of the fourth amendment than me. I think it needs to be respected and revered in every way. But this is not a fourth amendment issue; this is a national security issue. We need to change the law in such a way that our military protectors and defenders, if they have intelligence that says that someone is trying to hack into the air traffic control system because they are working for the Libyan government or the North Korean government or the Iraqi government, and there is evidence in State and local criminal records that would help them find that person and stop them, we need to empower them to do that. The legislation that I will be proposing will do just that.

Mr. Speaker, the gentleman from Pennsylvania (Mr. WELDON), the chairman of the Subcommittee on Research and Development, and I have both served in local government; and we understand that one of the things that happens in local government is that for a long time people will say, there really needs to be a traffic light at such-and-such an intersection; it is really dangerous. And they come out to meetings and they tell their mayor and they tell their council and they talk for years about the need for a traffic light. Then, in places where government is not very responsive, which is not true in Delaware County, Pennsylvania, and it is not true in my area either, in places where government is not responsive, they do not put up the traffic light. They wait until there is a fatality, a fatal accident at that intersection, and then they rush and put the traffic light up.

I never want to come to this floor and have 435 Members clamoring to pass legislation that would unlock the potential of our military people, consistent with our Constitution; I never want to have them coming to this floor clamoring to do that because the morning news is full of reports of planes crashing over the sky over a major airport, or thousands of people being poisoned because their drinking water was poisoned and the computer systems that would have told the utility that were hacked into.

□ 2245

I never want to have a national uproar because all the 911 calls for a major city went to a pizzeria or an airline reservation counter instead of to the police and the fire department. I never want to have a situation where there is financial chaos and there is a run on our banks because the checking account records or credit card records of millions of Americans are deliberately sabotauged.

Mr. Speaker, this is not the stuff of a Tom Clancy novel. It is the stuff that Members of this House are hearing about, both in classified and unclassified briefings. We have been warned, and to the Paul Reveres of this effort, like the gentleman from Pennsylvania (Mr. WELDON), the gentleman from South Carolina (Mr. SPENCE), and the gentleman from Missouri (Mr. SKELTON) who have paid attention to this, Secretary Hamre, people that work with him, we need to give them the tools that they need to continue to do this job.

I notice that my friend, the gentleman from Pennsylvania (Mr. WELDON) is here. I am happy to yield to him, and commend him on his leadership on this for many years.

Mr. WELDON of Pennsylvania. Mr. Speaker, I thank my colleague and friend for yielding. I came over for this special order, having watched his beginning and agreeing totally with the statement, and I appreciate the gentleman's leadership in making this a personal issue for him, for taking the time to understand a very complicated issue that many Members do not have the time to get into, but which is so vitally important to our country.

As the gentleman knows from hearings that we have held in our Subcommittee on Military Research and Development, we are going through a major revolution in America that the people really do not understand. In fact, we only have had one other revolution of this kind in our country's history. It was when we changed from an agrarian country where we made most of our living on the farms and on the land to an industrial economy, where people went to work in our factories building products and materials. It was a difficult change for America, but we did it because we wanted to lead the world economy in the 1900s, and we did it very successfully.

Now we are going through a similar revolution, changing from an industrial economy to an information economy, where more and more every day in our lives we are affected by the use of computers and information technology.

As a result, some very interesting and difficult challenges face us, because the single biggest technology, probably, to improving our quality of life has been the use of information technology.

I would argue, and I think my colleague would agree with me, that the single biggest vulnerability to continuing our quality of life is the use of information technology. If an adversary wants to take out America, they know in most cases they cannot match us gun for gun, tank for tank, plane for plane. That is an impossible task. But they know full well that our society is largely dependent upon information systems: our military systems, our smart weapons; but even beyond that, our information systems. Our banking, our communications, our air traffic control, electric grid, are all based on information technology.

So if you are an adversary of the U.S. in the 21st century, you are going to try to find a way to neutralize that

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H977 2002

technology advantage, to level the playing field. That is exactly what nations are doing today. As my colleague knows, in classified hearings we have held, there are in fact countries today that are working very diligently in finding ways to be able to shut down the communications and information systems of America during times of conflict.

It is a major concern for us also because we are having a difficult time keeping talented young people in the service when they can make three to four times the amount of money they are making as a software engineer for the Pentagon going out to work for a private company. So we have a very difficult challenge keeping up with that technology leap.

In fact, in the past, in the history of the country, military technology has often been ahead of the civilian community: the first airplane, the first jet engine. That is changing now. With the growth of the information revolution, the private sector and information technology companies and some of our would-be adversaries have the technology capability equal to or better than we have in the military. Therefore, we have a tough time keeping up.

So the kinds of ideas that the gentleman is pursuing, the kinds of strategies to focus the attention of the American people, not just our military, on information vulnerability are critically important.

I will give the gentleman a couple of horror stories. I cannot give the details. But to highlight the point he has made, we had a classified hearing several years ago where it was documented to us that one of our military hospitals had all of its health care records, all the blood types of all the patients, changed by a hacker who broke into the IT system without the administration of the hospital knowing all the blood types had been changed.

If the American citizen sitting at home wants to understand the impact on their life, imagine a loved one being in the hospital and all of a sudden, every blood type of every patient has been changed by someone who had access to that information system.

The banking system in America likes to pride itself on being the best at information security, but we all know there was a New York bank just a few years ago that had $10 million illegally transferred out of its accounts by a St. Petersburg, Russia firm that they were not able to stop, and the banking community has had examples like that where hackers have broken in and taken money away.

As the gentleman has pointed out, we need to think differently in the 21st century. If a terrorist group comes into America and wants to discharge a chemical or biological weapon, we need to have broad-based data systems so we can detect whether or not there is a pattern of occurrence of health care problems that might indicate to us that someone has released some type of toxic material. Because a warning may not be accompanied by a bomb, it may simply be a low-key release of an agent that we will not be able to determine unless we have processes in place to be able to do massive data mining.

I want to also applaud my colleague because he has been assisting very aggressively in establishing the first smart region in America. The idea behind this initiative, the HUBs project, is to link up as many of our institutions in the four States of New Jersey, Delaware, Pennsylvania, and Maryland to demonstrate that we can build smart regions in America, we can link technology, but we must build security in the process. We must have encryption capability, we must have security controls and access controls, not just in the government agency systems but also in our hospitals, in our schools, in our colleges, in our private business establishments.

I just want to add my comments and my praise. The gentleman is a leader in this effort. I look forward to the legislation that the gentleman is working on. As I have told the gentleman, I would be happy to cosponsor it. We need forward thinking, because this is really a new challenge. It is the single biggest threat to our security in the 21st century, the threat of being able to disarm America's economy and America's quality of life by disarming our information systems.

Mr. ANDREWS. I thank my friend, and again, long before this was an issue on the evening news or the front page of the newspaper, the gentleman from Pennsylvania (Mr. WELDON) was working on this issue on his committee, on the floor.

It is not a partisan issue, it is an issue that he has played a major role in educating people about. We thank the gentleman for that, and I look forward to following the gentleman's lead and to bringing legislation to this floor this spring that will help address these issues.

Mr. WELDON of Pennsylvania. I look forward to supporting it. The gentleman mentioned bipartisan. He is so right. The gentleman mentioned John Hamre's name. There is no one I respect more in this administration than John Hamre. It is unfortunate that he is leaving to go head the Center for Strategic and International Security, but he is a great leader.

It was John Hamre who 2 years ago, in leading this administration on this issue, made this quote: "It is not a matter of if America has an electronic Pearl Harbor, but when."

This past year when he came in before our committee, he said that we were at war, in a cyber war, at the very moment he came in, because we were in the middle of a massive attack on our defense information systems by an organized network that we think was focused in a selected few countries, but it has been a totally bipartisan effort.

The gentleman's leadership has been critically important. There is a need for more work like the gentleman is doing, and again I look forward to supporting the gentleman's legislation.

Mr. ANDREWS. I thank my friend for being here tonight as well, Mr. Speaker. We are going to summarize.

I want again say that each one of us involved in this effort is devoted to the idea of our constitutional principles, devoted to the idea of the separation of civilian and military; of the fact that in this country, the military responds to decisions by the civilian sector.

Each one of us is firmly committed to the sanctity of the constitutional rights of privacy, the protection against search and seizure, the rights of legitimate people in our country to be protected from the abuse of State power. We need not choose between forfeiting our Fourth Amendment rights and defending our country. These are consistent goals.

But in order to pursue these goals, we need to rethink the way we pursue them. I think that is so very, very important.

Mr. Speaker, I am here late tonight, and normally I would have the greatest privilege of my life, which is tucking my 7-year-old and 5-year-old into bed, my daughters Jaqueline and Josie, and their mother did that a while ago, I hope, tonight.

We are really fortunate that we put our children to bed tonight in a country that is safe and streng. It is not safe and strong everywhere, there are children who are going to sleep tonight in horribly violent neighborhoods and areas and horribly violent homes, ruined by alcohol and drug abuse and by all kinds of pernicious behavior.

But this is a country that, at least in terms of pernicious behavior in the world, is safer than it has ever been, and is the safest place in the world because of those who sacrificed in the service of their country, and who do so tonight.

But despite that sacrifice, there is a war going on tonight. As we put our children to sleep tonight, we have to put them to sleep with the sure understanding that there are evil and pernicious people in the world who are trying to do to us what Hitler and the Japanese could not do to us with their bombs and their armaments in World War II, could not do to us what the former Soviet Union threatened to do with us with their intercontinental ballistic missiles in the Cold War, could not do to us what foreign powers have tried to do to us throughout our history. That is to undermine and destroy the sovereignty and sanctity of our country. The way they are trying to do it is pernicious, it is lethal, but it is very quiet.

I pray that the night will never come when we wake up and hear that millions of our fellow citizens have been poisoned by their drinking water because the software that is supposed to detect poison was hacked into.

I pray that we never wake up and hear that thousands of people crashed

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H978 2002

to their death above airports because of an intentional violation of our air traffic control system.

I pray that we never wake up and find financial chaos, and people withdrawing their money from our banking system because the money they thought was safe and the records they thought were accurate proved to be neither.

I pray that we never wake up to a country where, when we try to call our police and fire and emergency management personnel by dialing 911, we cannot get through because someone has deliberately interfered with that system.

This is a reality. Now, thankfully, it is a reality that our military and our intelligence community are preparing vigilantly to protect us against. It is our job to give them the tools. But there is immense preparation that still must be done on this floor in legislation with our resources to both require and incentivize our civilian sector to meet the same standards of protection as our military has met, and then to give our military and law enforcement the tools to apprehend those who do us harm.

Mr. Speaker, it is my prayer that this issue will become irrelevant because we will be so well prepared, but I do not assume that that is the case.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (Mr. HAYES). The Chair would remind all Members to address their remarks to the Chair and not the television audience.

ILLEGAL NARCOTICS

The SPEAKER pro tempore. Under the Speaker's announced policy of January 6, 1999, the gentleman from Florida (Mr. MICA) is recognized for half the remaining time until midnight, approximately 30 minutes.

Mr. MICA. Mr. Speaker, I come to the floor of the House again at this late hour to talk about an issue that I always try to address the House on Tuesday nights on, and that is the question or problem relating to illegal narcotics.

It has been several weeks. We have had some intervening business and time away from the House of Representatives, but some things have happened, and I wanted to report on my activities as chair of the Subcommittee on Criminal Justice, Drug Policy and Human Resources.

□ 2300

I also wanted to highlight some of the reports that have filtered through the media on this subject and bring my colleagues up to date on where we are and where we are going.

Since I last addressed the House, there have been some serious incidents in our Nation. One that has sort of riveted and focused the attention of the Congress and the American people was a situation with a 6 year old killing a 6 year old. The method was by a gun, and all the attention has focused on the gun. But like many of the other stories about tragedy in our society today, they fail to focus on the real problem, the situation that led to that tragedy.

In this instance, we had a 6 year old who, unfortunately, came from a crack house setting. The belief is that the father was in jail, a family without any normal nuclear bounds, and a situation where you had, I believe, a stolen weapon. No one focused that the root of the problem was, indeed, illegal narcotics, drug trafficking, drug addiction, crimes related to illegal narcotics.

I had an opportunity to conduct, at the request of Members, a hearing this past week when the Congress was in recess, traveled to Sacramento, the capital of California, and also down to San Diego to visit our joint agency task force operations in Alameda, California to see how our war on drugs and our problems with illegal narcotics in that area of the country are progressing.

The story I heard in hearings in California was as horrible as the death of this 6 year old, but magnified many, many times in stories of deaths of young people that I had never heard of and I am sure the American people had not heard of.

We had testimony by a lady by the name of Susan Webber Brown on one of the occasions of hearing, and I believe this was the one in Sacramento. Susan Webber Brown, who is involved with a program out there to help drug-addicted families, gave us some incredible and powerful testimony.

She talked about a 15 month old who overdosed on methamphetamine in Rancho Cordova. That is a 15 month old. A 5 month old tested positive for methamphetamine and succumbs to death with 12 rib fractures, a burned leg, and scarred feet by a methamphetamine addict in Los Angeles, California. Not killed with a gun, but murdered by illegal narcotics.

She testified to a 13 month old who died of heart trauma, broken spine, and broken neck by a methamphetamine addict. She was also raped and sodomized. This was in the California high desert.

Susan Webber Brown testified about a 25-month-old Oregon toddler who overdosed on methamphetamine. She testified to us about a 2 month old who dies on methamphetamine, who had methamphetamine in her system in San Jose, California.

Another death that we did not read about or was not publicized was the 2 year old who ate methamphetamine from a baby food jar in Twentynine Palms, California; a 14 month old who drinks lye and water from a parent's methamphetamine laboratory, hospitalized permanently with severe organ damage in Fairfield, California; a new baby who died from mother's breast milk laced with methamphetamine in Orange County.

An 8-week-old, 11-pound boy dies from methamphetamine poisoning found inside a baby bottle in Orange County. An 8 year old watches and hears mom die in a methamphetamine laboratory in Oroville, California. A 6 month old overdoses, semicomatose, seizing, and hospitalized who drank methamphetamine from a bottle. A 4 year old who tested positive for methamphetamine, beaten and hair pulled out by the mom's boyfriend in Chico, California.

One of the worst stories that was told and video pictures presented at our hearing was of a young child, a young girl who was beaten and tortured by her parents who were both on methamphetamine. When they finished beating and torturing this child, Susan Webber Brown told a stunned audience that they basically scalded their daughter to death, high on methamphetamine.

Now, we have heard about a 6 year old killing a 6 year old with a gun, but we have not heard these stories of babies even younger being victimized. Hidden behind the other stories are the facts that this 6 year old, again, came from a home setting, if one could call it a home, of illegal narcotics.

I was absolutely shocked by the methamphetamine epidemic in California and the Midwest. I have held hearings in Washington, and we have talked about it. We have heard testimony here about it. But until one hears individuals, visits the locale, and sees firsthand the damage that has been done by methamphetamines, one cannot imagine the damage that has been done.

It is amazing that the President of the United States, it is amazing that the leadership of this country, it is amazing that the media of this country can focus on a tragedy like a 6 year old shooting a 6 year old, not focus on the root causes of that death and the deaths I have cited here.

In fact, we are now up to 15,973 drug-related deaths in this country. That is the 1998 count, and the count continues to skyrocket. Many of these are silent deaths, not making the front page, not being discussed in the talk shows or the subject of the root causes of the death and the tragedy, not coming forward or part of the discussion. But I intend to make it part of the discussion.

Methamphetamine production, trafficking, and use has increased in our rural communities and midsize cities, according to a published paper that came out January 26 this year. The report stated that lab seizures, the drug labs that were seized by the Drug Enforcement Administration, have increased sixfold in the past 5 years, from 263 seizures in 1994 to 1,627 labs in 1998.

We heard testimony, not only in Sacramento, but also down in San Diego about methamphetamine. We had law enforcement officials who brought methamphetamine to Sacramento and

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H979 2002

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H980 2002

Document No. 101

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [i] 2002

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ii] 2002