

before their trips—equipment that is checked thoroughly upon their return.

Chamber officials say they haven't been able to keep intruders completely out of their system, but now can detect and isolate attacks quickly.

The Chamber continues to see suspicious activity, they say. A thermostat at a town house the Chamber owns on Capitol Hill at one point was communicating with an Internet address in China, they say, and, in March, a printer used by Chamber executives spontaneously started printing pages with Chinese characters.

"It's nearly impossible to keep people out. The best thing you can do is have something that tells you when they get in," said Mr. Chavern, the chief operating officer. "It's the new normal. I expect this to continue for the foreseeable future. I expect to be surprised again."

Mr. McCAIN. First of all, could I say that is just unfair. They are not claiming to be experts on cyber attacks. They are claiming that there are issues of liability, issues of information sharing, and other issues that they believe will inhibit their ability to engage in business practices and grow and prosper. So to say that somehow they claim they are experts on cyber security, they are not, but they are experts on how their businesses can best cooperate, share information, resist these attacks, and come together with other people and other interests to bring about some legislation on which we can all agree.

There are 3 million businesses and organizations that are represented here, I say to my colleague, so it seems to me that we should continue this conversation with them, particularly on issues of information sharing and liability. But to somehow say "well, we talked to them, but we did not agree with anything they wanted to do" is not fair to those 3 million businesses. We are making some progress. But please don't say they portray themselves as experts.

By the way, they hacked into my Presidential campaign, which shows they really were pretty bored and did not have a hell of a lot to do. But, anyway, go ahead.

Mr. DURBIN. I am sure that wasn't the case. I am sure it was a fascinating treasure trove of great insights and information.

But let me just say to my friend from Arizona, I am asking only for a little humility on both sides, both in the public sector and the private sector, by first acknowledging, as our security advisers tell us, that this is one of the most serious threats to our country and its future, and we should be joining with some humility, particularly if you have been victimized, whether in your campaign or in your offices, to understand how far this has gone. The FBI, according to Senator WHITEHOUSE when he came to the floor, found 50 different American businesses that had been compromised and hacked into by the same type of operation. Forty-eight were totally unaware of it. They did not even know it occurred. What we are trying to do is to get these businesses to cooperate with us so that we

share information and keep one another safe.

At the end of the day, it is not just about the safety of the businesses—and I think it is important that they be safe—but the safety of the American people. This is really a serious issue.

Mr. McCAIN. Can I say to my colleague, first of all, to somehow infer that businesses in America are less interested in national security than they are in their own businesses is not, I think, a fair inference. But let me also say that what they want to do is be more efficient in the way they can do business.

For example, information sharing—as you know, there is a serious problem with liability if they are not given some kind of protections in the information sharing they would do with each other and with the Federal Government. So we want to make sure they have that security so that they will more cooperatively engage in the kind of information we need. That is a vital issue. That is still something on which we have a disagreement.

I have no doubt that the comments of the Senator from Illinois about how important this issue is are true. Nobody argues about that. But we have to get it right rather than get it wrong. The Senator from Illinois and I have been here a long time, and sometimes we have found out that we have passed legislation that has had adverse consequences rather than the positive ones we contemplated. By the way, I would throw Dodd-Frank in there. No company is too big to fail now. I would throw in some of the other legislation we have passed recently, which has not achieved the goals we sought.

That is why we need, in my view, more compromise and agreement. I believe we can reach it. I give great credit to both of our cosponsors of the bill, but please don't allege that this is "bipartisan" in any significant way. Most of the Republican Senators oppose the legislation in its present form. All Republican Senators understand the gravity of this situation and the necessity of acting.

Mr. DURBIN. I say to my friend from Arizona, I hope we get this done this week. I know it is a big lift, and it is a lot to do. But I believe the threat is imminent, and I believe it is continuous. If we don't find a way through our political differences to make this country safer, shame on us.

I believe Senator COLLINS is from the Senator's side of the aisle and is proud of that fact. So it is a bipartisan effort. She worked with—

Mr. McCAIN. It depends upon your definition of "bipartisan."

Mr. DURBIN. Well, it is clearly bipartisan with Senators LIEBERMAN and COLLINS. I also say that to raise the question of Dodd-Frank and appropriate government oversight and regulation—I suggest that we reflect on three things: LIBOR, Peregrine Investments, and the Chase loss of \$6 billion.

To say that we should not have government oversight of our financial in-

stitutions that dragged us into this recession we are still trying to recover from—I see it differently. We vote differently when it comes to that. I think there is a continuing need for government oversight of these financial institutions.

Mr. McCAIN. These institutions are not averse to government oversight. They are averse to legislation that harms their ability to share that information because if they face the threat of being taken into court for that, then obviously there is some reluctance. They also know how much has been lost because of the lack of cyber security to China and other countries. They are the ones who have been most directly affected. They are intelligent people, smart people, and they want this legislation to pass in a way that is the most effective way to enact legislation on this very serious issue.

I look forward to continuing the conversation with my friend from Illinois. I think both of us learn a bit from our conversations, and I thank him for his continued willingness to discuss the issue.

Mr. DURBIN. I thank my friend, the Senator from Arizona. I hope other colleagues will engage in this kind of exchange. I don't know if we convinced one another, but we certainly leave with the same level of respect with which we started. I hope those who have followed the debate have heard a little more about both sides of the issue in the process.

Mr. McCAIN. I yield the floor.

#### CORRECTING THE ENROLLMENT OF H.R. 1627

Mr. DURBIN. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of S. Con. Res. 55, which was submitted earlier today by Senator HARKIN.

The PRESIDING OFFICER. Without objection, it is so ordered. The clerk will report.

The bill clerk read as follows:

A concurrent resolution (S. Con. Res. 55) directing the House of Representatives to make a correction in the enrollment of H.R. 1627.

There being no objection, the Senate proceeded to consider the concurrent resolution.

Mr. DURBIN. Mr. President, I ask unanimous consent that the concurrent resolution be agreed to, the motion to reconsider be considered made and laid upon the table, with no intervening action or debate, and that any statements relating to the measure be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The concurrent resolution (S. Con. Res. 55) was agreed to, as follows:

#### S. CON. RES. 55

*Resolved by the Senate (the House of Representatives concurring), That, in the enrollment of the bill (H.R. 1627) an Act to amend title 38, United States Code, to furnish hospital care and medical services to veterans*

who were stationed at Camp Lejeune, North Carolina, while the water was contaminated at Camp Lejeune, to improve the provision of housing assistance to veterans and their families, and for other purposes, the Clerk of the House of Representatives shall make the following correction: in section 201, strike "Andrew Connelly" and insert "Andrew Conolly".

VETERANS JOBS CORPS ACT OF 2012—MOTION TO PROCEED—Continued

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. BLUMENTHAL. Mr. President, I am honored and grateful to follow that very enlightening and energetic exchange between two of the most able and respected Members of this body on a range of issues.

One of them I want to address now, and I want to particularly thank the Presiding Officer for his contribution, my distinguished friend from Minnesota, who has really addressed so instructively some of the privacy concerns in various proposals in an amendment I have joined. I think his work on that issue is really reflective of the approach that has been brought to this issue of cyber security—an issue that this entire body, in my view, has a historic opportunity and also a historic obligation to address this week, deal with it now authoritatively and effectively and in a way that the Nation expects us to do it.

I thank not only the Presiding Officer but a bipartisan group of colleagues, beginning with Senators LIEBERMAN, COLLINS, ROCKEFELLER, FEINSTEIN, and CARPER, who deserve our appreciation for drafting this bill and bringing it to the floor, and a number of other colleagues, including, along with the Presiding Officer, Senators WHITEHOUSE, MIKULSKI, COONS, COATS, BLUNT, AKAKA, and KYL. I mention this number because I think it is an important fact about the process that has brought us to this point. It really reflects the kind of collegial approach that is so important to this legislation.

This legislation has undergone very significant and substantial revisions to reflect suggestions made by myself and our colleagues, and this bill will give the government and private sector an opportunity to collaborate and share information so that they can confront the ongoing, present, urgent cyber threat directly and immediately.

This bill is not a top-down approach; it is voluntary in its direction to the private sector. What it says to critical industries—industries that are critical to our infrastructure—is that you determine what the best practices are, you tell us what the standards should be, and then those standards will be shared throughout the industry and overseen by a council that the Departments of Commerce and Justice and Defense and Homeland Security will be involved in implementing. And if companies comply with those standards—voluntary standards—they receive benefits that will enlist them in the program, benefits that will form incen-

tives in the form of limited immunity in the event of an attack. If companies decline to comply, if they are not provided with sufficient incentives, in their judgment, there is no compulsion, no legal mandate that they need to do so. To use an often overused imagery, what we are talking about here is a carrot, not a stick, in solving one of the most pressing and threatening challenges our country faces today. It is the challenge of this moment, the challenge of our time.

I have been in briefings, as has been the Presiding Officer and other Members of this body, with members of the intelligence community and others who have, in stark and staggering terms, presented to us the potential consequences of failing to act.

Just last week, GEN Keith Alexander, the chief of the U.S. Cyber Command and the Director of the National Security Agency, said that intrusions on our essential infrastructure have increased 17-fold between 2009 and 2011 and that it is only a matter of time before physical damage will result. He has said that the loss of industrial information and intellectual property—putting aside the physical threat and taking only the economic damage—is “the greatest transfer of wealth in history.”

We are permitting with impunity the greatest transfer of wealth in history from the United States of America to adversaries abroad, companies based overseas, at a time when every Member of this body says our priority should be jobs and protecting the economy of this country. It is an economic issue, not just a national security issue. In fact, cyber security is national security.

The United States is literally under attack every day. General Alexander described 200 attacks on critical infrastructure within the past year. He alluded to them without describing them in detail. And on a scale of 1 to 10, he said our preparedness for a large-scale cyber attack—shutting down the stock exchange or a blackout on the scale comparable to the one in India within the past few days—is around a 3 on a scale of 1 to 10. That situation is unacceptable.

We are, in a certain way, in a period of time now that is comparable to 1993, after the first World Trade Center bombing. Remember, in 1993 the World Trade Center—1,336 pounds of explosives were placed in a critical area of the World Trade Center, killing 6 people, injuring 1,000, fortunately, at that point, failing to bring down the building, which was the objective. That first bombing was a warning as well as a tragedy. America, even more tragically, disregarded that warning in failing to act. We are in that period now, comparable to 1993 and before 9/11, when the country could have acted and neglected to do so. We cannot repeat that failure now. We cannot disregard the day-to-day attacks, the serious intrusions that are stealing our wealth and endangering our security, our critical grid, transportation, water treat-

ment, electricity, and financial system. The scale of damage that could be done is horrific, comparable to what 9/11 did. We have an obligation to act before that kind of damage is faced in reality by the country.

We have been adequately and eloquently warned on the floor of this body, in private briefings available to Members of this body, and in the public press, to some extent. One of the frustrations I think many of us feel is that we cannot share some of the classified briefings we have received which would depict in even more graphic and dramatic terms what this Nation faces. Some of these attacks are launched by foreign countries that seek to do us harm. Some are launched by domestic criminals who simply want to steal money. Some are sophisticated and some are very crude.

Former Deputy Secretary William Lynch has detailed just one attack in which a foreign computer hacker—or group of them—stole 24,000 U.S. military files in March of 2011. As others have noted on the floor as recently as a few minutes ago, in late 2011 the computers of the U.S. Chamber of Commerce were completely compromised for more than a year by hackers. Yet today the U.S. Chamber of Commerce has essentially opposed the voluntary standards-based plan to help secure our Nation against attack. In fact, how extraordinary it is that certain parts of this bill have actually combined a consensus among the business community, the privacy advocates, as well as public officials, the National Security Agency. That consensus on privacy, again, reflects a profound and extraordinary feature of this bill, which is that we are coming together as a nation to face a common problem in a way that is demanded by the times and threats we face.

Shawn Henry, the Executive Assistant Director of the FBI, has said that “the cyber threat is an existential one, meaning that a major cyber attack could potentially wipe out whole companies.” That is the reason the business community has been involved and should support these proposals.

These attacks are not only ongoing, they have been occurring for years. These criminals are infiltrating our communications, accessing our secrets, and sapping our economic health through thefts of intellectual property.

Finally, Secretary of Defense Leon Panetta, as has been frequently quoted, said:

The next Pearl Harbor we confront could very well be a cyber attack that cripples our power system, our grid, our security systems, our financial systems, our government systems.

The panoply of harm is staggering, and we cannot wait for that harm to be a reality to this country. The consequences comparable to 9/11 are tragic to contemplate. FBI Director Mueller has said the cyber threat, which