Tarawa, Iwo Jima, and other destinations in the war against Japan during World War II.

For years, the U.S. naval officials pleaded earnestly for the United States to show presence in the South Pacific, and the suggestion was the harbor in Pago Pago on Tutuila island in the Samoan islands would be an ideal place to build a coaling station and a naval facility to allow U.S. naval ships and commercial vessels to utilize especially during the hurricane season.

In 1899, in Washington, D.C.—not known to the Samoans—the United States, Great Britain, and Germany held a conference whereby a tripartite treaty was agreed upon so that Germany and Great Britain would continue their colonial policies of figuring out how to control the two largest islands—Savai'i and Upolu—and the U.S. was free to deal with the traditional leaders and chiefs of the islands of Tutuila, Aunu'u, and Manu'a. And by consent of these chiefs, they ceded these islands to the United States in 1900 and 1904. These proposed treaties were never approved by the United States Congress until 1929.

□ 1640

Some ask today, Is a territory like American Samoa still relevant to our Nation? And to that I would argue, absolutely—especially given the U.S. pivot of focus on the Asia Pacific region, from our continuous involvements for over 10 years now in Iraq and Afghanistan.

Mr. Speaker, I would ask the question, What would happen if the leaders of Samoa or perhaps Fiji or Vanuatu or the Solomon Islands or Tuvalu or Kiribati would agree to have, let's say, China perhaps build a submarine base on these islands? I would be curious if our Department of Defense or the Pentagon or even the Congress might indicate some concern in this region of the world.

Mr. Speaker, as a Vietnam veteran and as a representative of a district with high rates of military enlistment, I respectfully urge the Senate to adopt the House provision that would give due honor to all of our servicemembers from the District of Columbia, Puerto Rico, Guam, the Virgin Islands, American Samoa, and the Northern Mariana Islands.

I thank my colleagues who have gathered here today. And with one voice today, we say, Do the right thing and honor the ultimate sacrifices of the tens of thousands of our men and women who proudly served the armed services of our Nation who are from our U.S. territories and the District of Columbia.

Mr. Speaker, I want to note for the record that I know that our colleague, the gentlelady from Guam who is also a senior member of the House Armed Services Committee, would have been here. But because of other commitments, she was unable to join us in this Special Order.

Mr. Speaker, in closing, I am reminded again of a statement made by a retired U.S. Marine brigadier general and a dear Republican friend of mine, a native Chamorro from Guam, a graduate of the University of Notre Dame and a very dear Republican friend, as I said, and former colleague of ours in Congress. He was a former Member of this House. He observed that in our relationship between our Nation and the Territories, he said, We are equal in war but not in peace.

With that, Mr. Speaker, I sincerely hope that our colleagues in the Senate, Chairman CARL LEVIN; the distinguished Republican Senator, the senior ranking member and dear friend as well, JOHN MCCAIN; and all the members of the Senate Armed Services Committee will support this provision.

And to the gentlelady from the District of Columbia, I cannot help but to say more. There are 600,000 U.S. citizens living in her district. They pay Federal income taxes, and yet she is denied the right to vote on the floor. I think this is something that is unbecoming of what we call ''democracy,'' if I will.

Ms. NORTON. You have heard movingly from three of my colleagues. I hope the Senate has been as moved as I was by hearing from them.

I want only to say now, Mr. Speaker, you've heard from all of us who are American citizens who represent American citizens and American citizens who fight and have fought for their country, who were pleased and continue to volunteer in disproportionate numbers into the Armed Forces, who are among the less than 1 percent, who carry all of us, who carry all of us on their shoulders. That's what the volunteer Army is all about today.

We've asked the Senate to do what we congratulate and commend and thank the House for having already done. Thank you, House of Representatives, for respecting our flags and for respecting us as representatives of the American people and of American veterans.

And I yield back the balance of my time.

BACK TO CONGRESS TO PROTECT THE HOMELAND

The SPEAKER pro tempore. Under the Speaker's announced policy of January 5, 2011, the Chair recognizes the gentleman from California (Mr. DANIEL E. LUNGREN) for 30 minutes.

Mr. DANIEL E. LUNGREN of California. Mr. Speaker, on 9/11, I was in the city and, therefore, was an eyewitness to the impact of the attack on the United States in the Capital City.

I had a friend who was on the airplane that was crashed into the Pentagon. There was a gentleman who was a partner in the law firm that I had just joined who was on that airplane. A young man who had attended school with my children and his family had worshiped at the same Catholic church was on the level hit by the first airplane in the Twin Towers.

And understanding the nature of the attack against the United States, at that time, I felt a strong urging to once again be involved in public service. And that was the genesis of my decision, when the opportunity presented itself several years later, to return to this body. That was the compelling reason.

I was privileged to be appointed to the permanent Homeland Security Committee, and I was privileged to serve as chairman of one of the subcommittees; and since that time, I have been privileged to continue to serve on that committee as well as to serve on the House Judiciary Committee where we had responsibility for, among other things, the PATRIOT Act and FISA, the Foreign Intelligence Surveillance Act, both of which were, in my judgment—and are, in my judgment—essential to our response to the threat that existed at the time of their creation and the threat that remains.

One of the ironies of my service is that I am elected from a district in Sacramento County, California, nearly 3,000 miles from the site of the attack in New York and the attack here in Washington, D.C. And while we have had a plot to blow up L.A. airport that was thwarted by tremendous work by a Federal employee on our northwestern border, it has been somewhat difficult to articulate in sufficient terms the threat that remains to us, as a Nation, to my constituency.

But those in California are not alone in their failure to understand the urgency of the moment. I think we, as a Nation, have, as a result of the successes that we have achieved in our defense of this Nation, allowed ourselves some level of complacency and a misapprehension of the danger that remains.

When I served in the Congress in my first tour of service from January of 1979 to January of 1989, I for several years was a member of the House Intelligence Committee. At that time, the phrase ''homeland security'' or the word ''homeland'' was never uttered. If you had uttered it then, it would have a foreign sense to it. Protect the homeland, wasn't that what Hitler was talking about? There was a strange notion to that term.

It, of course, began to be used in normal parlance after 9/11. And now it regularly trips off our tongues, ''homeland security,'' ''the Committee on Homeland Security,'' ''the defense of the homeland,'' because we understand that the nature of the war in which we are presently engaged is very different than the wars that we have engaged in in the past.

Those were wars of territorial conquest. Those were wars where you could gauge success or failure by the amount of territory that you had taken, by the number of people who had died, by the men and armaments that were proceeding into battle. And

in some ways, you could anticipate the success or failure by the location of the troops, by the array of weapons.

Today we're facing a very different threat. In addition to fighting the war that has gone on in the Middle East—with our men and women in uniform performing bravely and as well as any that we have ever had—we are now dealing with an enemy that is not defined as a nation-state solely, is not defined as a physical army moving to our shores but is in many ways engaged in the essence of asymmetric warfare. That is, not pitting one military force against a military force, one grouping of military equipment versus another but, rather, the essence of asymmetric warfare in attempting to create psychological more than physical damage but physical damage if they may do so.

□ 1650

On 9/11, we suffered tremendous physical damage. We lost over 3,000 people. We saw one of the symbols of American capitalism destroyed, one of the symbols of American free enterprise, one of the symbols of one of America's greatest cities. We also saw an attack on the Pentagon. It didn't destroy the Pentagon. It didn't cause the number of casualties you would see in a major battle, although every life lost was a tragedy; but it was a psychological blow to the United States. It was in some ways the foundational principle of terrorism.

How do you exact the greatest amount of terror, a lack of confidence, a fear in a people, particularly in the civilian population, while doing what would be, relatively speaking, a small amount of damage? I don't want to diminish the amount of physical damage that was done, but relative to the scenes that we have seen from World War II for destruction of entire cities, for destruction of buildings and infrastructure that existed not for years, not for decades, but for centuries. Yet, the threat is as great as the threats we have faced before.

Within the context of this war of terror, as opposed to the war on terror, because the war is really against those who would destroy us utilizing terror, I don't think you should define a war as against the tactics used by the enemy. You have to define the enemy. We've had some difficulty in doing that in part because of political correctness, but an essential part of this war on terror is found in the world of cyber. That's what I would like to address this evening for a few moments, cybersecurity.

I think one of the great failings of this Congress and one of the things that I regret having not accomplished before I leave this House in several weeks is our successful addressing of the threat we find in the world of cyber. The cyberworld is difficult to grasp because you can't smell it, you can't feel it, you can't touch it, and you can't hear it. Yet it is embedded in virtually everything we do. If you would look at the world of computers, the world of technology, the world of connectivity of those things, and the wireless world—that is a term that needs to be defined, and we don't have the full time to talk about that because wireless means partly wireless instrumentalities and partly wired instrumentalities and partly cables, which are utilized to spread what started may end as wireless communications to distant lands. Nonetheless, because you can't physically see it in most instances, it is not readily apparent that it is there.

While the essence of this new computerized technology-connected world allows us to do things we never dreamed of doing before, and while that enhances our standard of living and permits us to be able to receive goods and services and specific essential communications instantaneously from far away places, it also creates tremendous vulnerabilities. To the extent that you are connected, you're also vulnerable. To the extent that you rely on that connectivity to be able to send control decisions to distant places, you also create a vulnerability along that pathway; you create a vulnerability for someone who might be able to capture that control.

And as you understand the place that the cyberworld plays in our critical infrastructure, that which gives us the guts of the underpinnings of our standard of living—power, electricity, water, just to name a few—you understand if someone controls those or interferes with those or sends off false messages on those, the world as we know changes. And if those who control in that way by hacking, by intervention, by malware, if they are successful, they change our standard of living tremendously, and not for the better.

What do we have to do? In the first instance, we have to recognize the problem. In this body, we've not recognized that problem. In the Senate, they have not recognized that problem. With all due respect, even though I work very closely with the administration, it hasn't been priority enough. The public doesn't understand it or appreciate it in part because it is not a politically sexy thing to talk about.

I grew up in southern California where a news director many years ago coined the phrase ''if it bleeds, it leads,'' meaning we will put it on TV if you can find a car crash. You find somebody bleeding somewhere, we'll put it on TV long before we'll put some good that someone has done on TV. Cybersecurity doesn't bleed until someone invades it, someone captures it.

One of the remarkable things that happened over the last couple of years was something called Stuxnet, S-t-u-x-n-e-t. Stuxnet is an example of—I'll call it malware or a virus or whatever you want to call it. It was an intrusion into an already-existing IT system, the Iranian Government's system that they utilized for purposes of developing their nuclear weapons systems. At least that is what is suggested in the public press.

According to the public press, whatever this was that was interjected there laid dormant for a period of time, gave off false signals that everything was okay to those who were operating the system, and then at some period of time carried out commands that were contrary to the integrity of the system, causing, as reported in public articles, the centrifuges in their nuclear system to basically destroy themselves.

Why is that important? It was the first example we've seen publicly of a physical destruction of a system. I would call that in the nature of critical infrastructure as a result of a cyberattack. We've seen suggestions of other such things. Whoever did that, thank God they seemed to be on our side. But now the genie is out of the bottle. And if it were done by those who are friends of ours, what would happen if people captured it that were not friends of ours? Now that it has been done successfully, evidently they know it can be done. So you can have people who try and reverse engineer it, or you can have people just start from ground zero saying, look, it has been done, let us now theoretically determine how it was done and how we can do it. My point is once it has happened, we should understand that there are those who want to destroy us that will use it against us.

Let me ask a question, and that would be: What would happen if someone introduced malware or viruses into several of the major medical or health systems in this Nation? If you went to the hospital and instead of you having accurately recorded what your blood is, you had another blood type and you're going to need a blood transfusion during that surgery, what if they were able to change the indications you have for indications or the contraindications that you have so you would be subjected to medicines that were not, in fact, good for you?

□ 1700

What if that happened in a couple of major health systems in this country in different parts of the country? Would that be a psychological attack on the Nation if we shook the confidence people had in the system? What if they were able to invade a financial services operation so that your account could not be verified and someone else's account couldn't be verified? What if, in fact, they controlled some of the systems that deal with our trains so that trains would be colliding rather than missing one another? What if they controlled the critical infrastructure that we call our water systems or our electricity delivery systems?

I mean, these are real questions. What do we need to do? We need to understand that it's going to require cooperation and a collaboration between the public sector and the private sector.

Look, I'm a small-government guy. I believe in limited government. I also believe that the limited government we have ought to work, that it ought to be robust. In my judgment, the Federal Government has a responsibility in the area of cybersecurity; and we have been, in some ways, not facing up to that. This administration and the previous administration have done some tremendous work in advancing the cause—Congress has examined it; we've held hearings; we've put forth some proposals—but we haven't had a completed project. We need to do a number of things, it seems to me.

Number one, we need to make sure that we understand that, as far as the Federal Government is concerned, the entry point for the private sector ought not to be NSA, because it's part of the military. It ought to be DHS. Some people say, I didn't like DHS. Well, DHS exists. It has for a decade. It has gotten more robust. It has gotten much, much better in terms of its competency in the area of cybersecurity. We ought to build on that. We ought to have that as the entry point so that we don't have a violation of what we know as posse comitatus, or the idea of civilian control over the military.

NSA is unbelievably good. They're the best in the world at what they do, but we've got to make sure that there is the proper relationship. I think the previous administration and this administration have established the means of doing that, but it ought not to be the idiosyncratic answer by one administration to another. It ought to be institutionalized so we know that that's the permanent structure and that people can rely on it.

Secondly, we need to create a platform of trust and confidence and experience between the public sector and the private sector to be able to utilize the information that comes to one or the other. What do I mean by that?

When the Federal Government learns about cyberattacks that are taking place in one place, they ought to be able to give that information to other elements of the private sector on an immediate basis so they can protect themselves against that. At the same time, we ought to set up a platform to establish that confidence so that the private sector will feel better about giving their information to the government so that they can help them protect against that attack and let others know that that attack might be there. That comes with experience. That comes with trust and confidence that can only be established over time, and we need to have a structure that allows that to happen.

I produced legislation to do that. Unfortunately, it never reached the floor of the House of Representatives for reasons I won't go into, but the fact of the matter is that we still need to do that. You can say you want to build trust by establishing something, but you have to have it established. You have to have people there. They have to understand one another. They have to work with one another. They have to gain that trust. That takes time. We need to do it immediately.

We need to have some sort of means by which we work with the private sector that involves itself in critical infrastructure in such a way that the impact of a failure of that piece of infrastructure to the public will be protected against. Let me give you a simple example. This was an example that I paraphrased from former Secretary Chertoff.

Let's say you are a piece of the critical infrastructure and that you realize that a failure will cause $1 billion worth of damage to your company, but that the impact on society may be $50 billion. The delta between $50 billion and $1 billion is one that has to be, in some ways, dealt with in terms of that relationship between the Federal Government and the private sector; and we haven't figured that out yet.

My way of doing it was to create a voluntary program by which you would have different elements of our economy deal with DHS, with the support of others, coming up with what would be best business practices. Then, if those best business practices were adopted by those within that element of the economy, they would get liability protection, liability immunity. Now, some say, wait a second. That leads to the slippery slope, and the Federal Government is going to come in with a crash on you. Look, I don't know the perfect answer, but I was trying to find the lightest regulatory touch we could have.

If those who are worried about the Federal Government becoming too heavy handed are truly concerned about that, they ought to think about this: if we have a successful cyberattack against a part of our critical infrastructure, my fear is that Congress and whoever is President at the time will overreact because the public will require it. Wouldn't it be better for us to anticipate it? Wouldn't it be better for us to get ahead of the crisis and then have a means by which we defend against it? We know we're not ever going to be totally, 100 percent successful; so when it happens, we should diminish the impact on whatever part of critical infrastructure we have.

Third, mitigate against the damage when it occurs; and, fourth, be available to rebuild, respond and have the services available to the public sooner rather than later.

I had hoped to be here another 2 years to work on that—I will not be—but I will be on the outside, wherever I am and in whatever I do, urging this Congress to look this issue squarely in the face and to do something about it. I am absolutely convinced, as Secretary Panetta said, that one of the greatest threats to this Nation is a cyber-Pearl Harbor, and the potential of that is greater because the capacity to strike against the country is more diffuse than ever before.

The capital investment for a successful cyberattack is much less than the capital investment needed for weapons of mass destruction. We ought to understand it, and we ought to understand that sooner rather than later. Cybersecurity ought to be an issue on the front burner of this Congress going forward. There ought to be an effort for the administration and the Congress—Democrat, Republican, conservative, liberal—to work for the good of this Nation.

I can think of no external threat that is greater than the threat of cyberwarfare. As I leave this place, I don't know if I'd call it a confession, but it is an admission of mine that we have not done all we've needed to do. I'm not blaming anybody. In the aftermath of 9/11, the first thing we had to do was to try and protect against a similar attack. We have strengthened our air travel in this country. We have strengthened our security against an attack to our ports. We have strengthened our ability to protect against a terrorist attack on our chemical facilities, although we still need to do more there. We have protected our transportation systems to a greater extent than existed before. We have greater cooperation and coordination among all levels of law enforcement. There is a greater level of respect among the private sector parts and the public sector; but cybersecurity remains, in my judgment, the lagging indicator and the lagging response.

I would hope that partisanship would be thrown aside. I would hope that fear of the government—although I understand that well and I've been a proponent of that—of an overly sized government and an overly strong government will be tempered in the sense that we understand the threat to all of us and to our standard of living in so many different ways is real and that, right now, we have the greatest minds working on cyber.

The last thought is this: if any young person is looking for a job or a career for the rest of his or her life, start training in the area of cybersecurity. We need to do more in terms of our educational programs. We need to do more in terms of our training. China is training a lot more people in cybersecurity than we are. It's not just because they have a larger population; it's because they're dedicated to it. We could lose our edge if we don't do that.

So I would ask this Congress going forward and I would ask this administration going forward to put cybersecurity at the front of the line, not at the back of the line, in terms of training our people, educating our young people, identifying this as a career path for so many of them, making the commitment in our government in terms of the budget that is necessary, but also in terms of that spirit of cooperation and collaboration that must exist between the private sector and the public sector.

□ 1710

We are at risk. There is a real and present danger out there. We have the capacity to respond to it. We have the ability to be the best in the world at this. We have the ability to protect ourselves better than any other country in the world, and we will if we will turn our face towards the problem rather than away from the problem.

So, Mr. Speaker, I thank you for the time. It is my hope that this country recognizes the threat, deals with the threat, and successfully looks to the future for ourselves, our children, and our grandchildren.

I yield back the balance of my time.

REMEMBERING DAN McKINNON

The SPEAKER pro tempore. Under the Speaker's announced policy of January 5, 2011, the Chair recognizes the gentleman from California (Mr. HUNTER) for 30 minutes.

Mr. HUNTER. Thank you, Mr. Speaker.

It is my unfortunate honor to come before you and speak about a true son of America who lost his battle with cancer 6 days ago on November 22. I have an article here from the local paper in San Diego talking about Dan McKinnon, and it says, Dan McKinnon: Navy pilot, radio, and airline executive. Appointed to two Federal boards, was son of San Diego congressman. Those are a lot of things, but Dan McKinnon was so much more than those, even put together.

First, his father was a Democrat congressman from San Diego here in the 1950s, probably stood at this table and spoke like I'm speaking now. Dan was a page, when we still had pages in this House on this floor in the fifties during the Truman administration as well. He had a great respect and love for this country, and he had a great respect and love for this body and the institution.

He has some great claims to fame. One of those is this: As a young man, Dan served in the Navy as a helicopter pilot, and he's credited with 62 saves on land or sea. That's more saves during peacetime than any other Navy pilot in American history. He loved the Navy and he loved flying, and that led him to do other things later in his life. But he was a great pilot. He was inspired to fly from some words taken from the movie ''The Bridge Over Toko-Ri.'' And basically the words—I'm going to summarize what made him want to be a helicopter pilot. There were some folks talking in this movie, and they basically said: Where does America get these kinds of people that want to fly off these little platforms that are floating in the ocean, go and rescue men or take out the enemy, and then fly back out to these platforms again in the middle of the ocean, try to find those platforms and then land on them? Where does America get them? They are the greatest in that country.

That inspired Dan to join the Navy and do exactly that—to fly helicopters and rescue his fellow sailors that had the bad luck or the bad skills to land in the water.

He bought a country radio station in San Diego and transformed it, made it into one of the most successful radio stations in San Diego County. At the same time, in 1977 he was the president of the Country Music Association in Nashville. He also served on the National Association of Broadcasters' board of directors here in Washington, D.C.

And as I go through this litany of things that Dan McKinnon did, you can see where his courage, his faith in God, and his selfless service to country and Christianity played through throughout his entire life.

He ran for Congress. He tried to get in this body in 1980. He had an unsuccessful run for Congress in 1980, but the next year President Reagan nominated him to lead the Federal Civil Aeronautics Board which basically oversaw the deregulation of all of the airlines. And as I know, as somebody who wants less government and less Big Brother intervention, Dan McKinnon was the rare sort of man who, after he did his work on the Civil Aeronautics Board and deregulated the airline industry, so we have what we have now, which is competition and low rates and extremely high safety measures, he shut down his own board that President Reagan started. Rarely in Washington do you see a creature that starts up some kind of board or blue ribbon panel or commission and actually closes it down on themselves after they've done the work that they needed to do. That takes a special person. It takes a special person to give up the reins and say, we don't need more bureaucracy, we're going to shut it down. We've done the work that we were assigned. So he did that. He didn't get paid for that either. He did it because he wanted to help the country and he loved being a pilot and he loved the airline industry.

People say that the airline industry right now, the way that it is is a direct reflection of how he deregulated it during these times. That was a big deal when you had the Federal Government dictating fares and routes, and to change that into a free market system where competition could enter, it took a long time and it took a man of special character and significance to do that, and Dan did it.

His daughter Lisa, who is, I think, a lieutenant in the Navy right now in Coronado doing intelligence work for the Navy SEALs, said this about her dad: He would say that his Navy wings were the only thing that he ever did by himself. He said everything else was a team effort. He loved being a pilot. He loved flying for the Navy, and he flew and sailed to the end of his days.

He also worked for the Central Intelligence Agency. They had him doing special projects, and he actually got the Seal Medallion from the Central Intelligence Agency.

So you take all of these things together, and you see a man who had a full life, a full family, that loved his country and served his country, and someone who had courage and true grit and a true faith in God, that God would help lead him through his life and his path, and he trusted in the Lord to do that.

On a couple of other separate stories, Dan taught me how to jump motocross bikes at his ranch when I was a kid. I got my first job in high school at a TV station doing the news camera that his brother had. I got to work on his airlines after high school and between college. I'm a young guy. I'm only 35 years old, Mr. Speaker, and sometimes young guys like myself need people to look up to, people that give us structure and people that tell us which way is the right way to go and which way is the wrong way to go. Dan always knew what the right way to go was. He was a mentor of mine. And on November 22, when he lost his battle with cancer, America and San Diego truly lost one of their sons and one of the people that make this country truly great.

With that, I yield back the balance of my time.

RECESS

The SPEAKER pro tempore. Pursuant to clause 12(a) of rule I, the Chair declares the House in recess subject to the call of the Chair.

Accordingly (at 5 o'clock and 17 minutes p.m.), the House stood in recess.

□ 1739

AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Mr. WOODALL) at 5 o'clock and 39 minutes p.m.

REPORT ON RESOLUTION PROVIDING FOR CONSIDERATION OF H.R. 6429, STEM JOBS ACT OF 2012; AND PROVIDING FOR CONSIDERATION OF MOTIONS TO SUSPEND THE RULES

Mr. NUGENT, from the Committee on Rules, submitted a privileged report (Rept. No. 112–697) on the resolution (H. Res. 821) providing for consideration of the bill (H.R. 6429) to amend the Immigration and Nationality Act to promote innovation, investment, and research in the United States, to eliminate the diversity immigrant program, and for other purposes; and providing for consideration of motions to suspend the rules, which was referred to the House Calendar and ordered to be printed.

SENATE BILL REFERRED

A bill of the Senate of the following title was taken from the Speaker's table and, under the rule, referred as follows:

S. 3642. An act to clarify the scope of the Economic Espionage Act of 1996, the Committee on the Judiciary.