U.S. Department of Defense
Office of the Assistant Secretary of Defense (Public Affairs)
Speech

On the Web:
http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728
Media contact: +1 (703) 697-5131/697-5132

Public contact:
http://www.defense.gov/landing/comment.aspx
or +1 (703) 571-3343

"Defending the Nation from Cyber Attack" (Business Executives for National Security)
As Delivered by Secretary of Defense Leon E. Panetta, New York, New York, Thursday, October 11, 2012

Thank you. Thank you very much. Thank you so much for this wonderful evening and the chance to enjoy such terrific company and be able to express my deepest gratitude to this organization for all of the great things that it does on behalf of those that serve in our military.

Bruce, my greatest thanks to you for your kind remarks and for your leadership here. And I -- I accept this award, not so much for myself but I accept it on behalf of the men and women in uniform who are putting their lives on the line every night, every day in order to protect this country.

I want to congratulate the troops from the 82nd, they're -- they're the very best. I also want to congratulate Frank for receiving this reward, the great service that he does in helping to -- to find jobs for those that are returning so that they can be part of -- of their community after serving this country, to protect their community is outstanding. And besides that, and perhaps most importantly, he's Italian. It's nice to have another Italian honored this evening.

I also want to thank Fran Townsend. She's a great friend and, obviously, a tremendous Master of Ceremonies this evening. And the reason I -- the reason I asked Fran to serve on the board is because she is bright. She is capable. She's dedicated. She -- she's a straight talker, she knows what she's talking about. She's dedicated to this country and in a room of a lot of ugly old guys, she's not bad to look at. General Meigs, thank you for your leadership as well and for your distinguished service to this country.

I am truly honored to be with you this evening. We gather in the midst of a very important national contest. It's one that will continue to play out over the coming weeks in unpredictable ways before a final decision is reached. And in fact, some of the key players are dueling tonight. So I want to be very clear about where my loyalties lie in this contest, I have always been and always will be for the New York Yankees. And I think the score is 1-to-1. Right?

In all seriousness, I really do appreciate the opportunity to come back to this great city. This is -- New York is a special place for me and I'll tell you why. I am -- I'm the son of Italian immigrants and both of my parents came through New York, came through Ellis Island like so many millions of others. That made this a special place for me.

I also had the opportunity to be here and work as an Executive Assistant to the Mayor of New York City, a guy named John Lindsay at the time. I also had the opportunity to work very closely with the delegation in Congress. As a matter of fact, in Washington. I lived with Chuck Schumer and a group of other members of Congress in what was well known as Animal House in Washington. And you can't live with Schumer and not develop an appreciation for New York City.

I also served on the Board of the New York Stock Exchange for six years. And I was on the board when 9/11 took place and I want you to know how much at that time I appreciated the great courage of the people of New York in the face of that attack. And I remembered that courage when I had a chance to lead the operation that went after Bin Laden. We sent a very clear message to the world. We sent a very clear message to terrorists that in fact, don't ever attack this country because you will not get away with it.

I've long appreciated, from my own experience, New York's role as the center of gravity for our nation's economy. This is where it's at. And for that reason, it's an honor to be able to speak before this kind of distinguished audience of business leaders and innovators because you understand what a strong national defense is all about and you understand that a strong national defense and a strong economy go hand in hand.

With that in mind, tonight I'd like to discuss with you an issue that I think is at the very nexus of business and national security: the threats facing the United States in cyberspace and the role that the Defense Department must play in

defending this country from those kinds of threats.

We're on an aircraft carrier, a famous and great aircraft carrier and it's a fitting and appropriate venue to have this discussion. This ship and the technology that's on display at this museum, attests to one of the central achievements of the United States in the 20th century, our ability to project power and strength across the land, across the high seas, across the skies and across outer space.

We secured those domains. Securing them helped ensure that they were used to advance peace and prosperity and were not used to promote war and aggression. It is with that same goal in mind, today we have to address a new domain that we must secure to have peace and prosperity in the world of tomorrow.

Cyberspace has fundamentally transformed the global economy. It's transformed our way of life, providing two billion people across the world with instant access to information to communication, to economic opportunities. Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers.

The Internet is open. It's highly accessible, as it should be. But that also presents a new terrain for warfare. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens.

I know that when people think of cybersecurity today, they worry about hackers and criminals who prowl the Internet, steal people's identities, steal sensitive business information, steal even national security secrets. Those threats are real and they exist today.

But the even greater danger -- the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states are violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.

Let me give you some examples of the kinds of attacks that we have already experienced. In recent weeks, as many of you know, some large U.S. financial institutions were hit by so-called Distributed Denial of Service attacks. These attacks delayed or disrupted services on customer websites. While this kind of tactic isn't new, the scale and speed with which it happened was unprecedented.

But even more alarming is an attack that happened two months ago when a very sophisticated virus called Shamoon infected computers in the Saudi Arabian State Oil Company Aramco. Shamoon included a routine called a ‘wiper’, coded to self-execute. This routine replaced crucial systems files with an image of a burning U.S. flag. But it also put additional garbage data that overwrote all the real data on the machine. More than 30,000 computers that it infected were rendered useless and had to be replaced. It virtually destroyed 30,000 computers.

Then just days after this incident, there was a similar attack on RasGas of Qatar, a major energy company in the region. All told, the Shamoon virus was probably the most destructive attack that the private sector has seen to date. Imagine the impact an attack like that would have on your company or your business.

These attacks mark a significant escalation of the cyber threat and they have renewed concerns about still more destructive scenarios that could unfold. For example, we know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country.

We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life.

Let me explain how this could unfold. An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches. They could, for example, derail passenger trains or even more dangerous, derail trains loaded with lethal chemicals. They could contaminate the water supply in major cities or shutdown the power grid across large parts of the country.

The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a “cyber Pearl Harbor:” an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.

As director of the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more

well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East.

And the cyber threats facing this country are growing. With dramatic advances, this is an area of dramatic developments in cyber technology. With that happening, potential aggressors are exploiting vulnerabilities in our security. But the good news is this, we are aware of this potential. Our eyes are wide open to these kinds of threats and we are a nation that, thank God, is on the cutting edge of this new technology. We are the best and we have to stay there.

The Department of Defense, in large part through the capabilities of the National Security Agency, NSA, has develop the world's most sophisticated system to detect cyber intruders and attackers. We are acting aggressively to get ahead of this problem, putting in place measures to stop cyber attacks dead in their tracks. We are doing this as part of a broad whole of government effort to confront cyber threats.

The Department of Homeland Security has the lead for domestic cybersecurity, the FBI also has a key part to play and investigating and preventing cyber-attacks. And our intelligence agencies, of course, are focused on this potential threat as well. The State Department is trying to forge international consensus on the roles and responsibilities of nations to help secure cyberspace.

The Department of Defense also has a role. It is a supporting role but it is an essential role. And tonight I want to explain what that means. But first let me make clear what it does not mean.

It does not mean that the Department of Defense will monitor citizens' personal computers. We're not interested in personal communication or in e-mails or in providing the day to day security of private and commercial networks. That is not our goal. That is not our job. That is not our mission.

Our mission is to defend the nation. We defend. We deter, and if called upon, we take decisive action to protect our citizens. In the past, we have done so thorough operations on land and at sea, in the skies and in space. In this century, the United States military must help defend the nation in cyberspace as well.

If a foreign adversary attacked U.S. soil, the American people have every right to expect their national defense forces to respond. If a crippling cyber attack were launched against our nation, the American people must be protected. And if the Commander in Chief orders a response, the Defense Department must be ready to obey that order and to act.

To ensure that we fulfill our role to defend the nation in cyberspace, the department is focusing on three main tracks. One, developing new capabilities. Two, putting in place the policies and organizations we need to execute our mission. And three, building much more effective cooperation with industry and with our international partners. Let me briefly talk about each of these.

First, developing new capabilities. DoD is investing more than $3 billion annually in cybersecurity because we have to retain that cutting edge capability in the field. Following our new defense strategy, the department is continuing to increase key investments in cybersecurity even in an era of fiscal restraint.

Our most important investment is in skilled cyber warriors needed to conduct operations in cyberspace. Just as DoD developed the world's finest counterterrorism force over the past decade, we need to build and maintain the finest cyber force and operations. We're recruiting, we're training, we're retaining the best and the brightest in order to stay ahead of other nations. It's no secret that Russia and China have advanced cyber capabilities. Iran has also undertaken a concerted effort to use cyberspace to its advantage.

Moreover, DoD is already in an intense daily struggle against thousands of cyber actors who probe the Defense Department's networks, millions of time a day. Throughout the innovative efforts of our cyber operators, we've been trying to enhance the department's cyber-defense programs. These systems rely on sensors; they rely on software to hunt down the malicious code before it harms our systems. We actively share our own experience defending our systems with those running the nation's critical private sector networks.

In addition to defending the department's networks, we also help deter attacks. Our cyber adversaries will be far less likely to hit us if they know that we will be able to link to the attack or that their effort will fail against our strong defenses. The department has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack.

Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.

But we won't succeed in preventing a cyber attack through improved defenses alone. If we detect an imminent threat of

attack that will cause significant, physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us to defend this nation when directed by the president.

For these kinds of scenarios, the department has developed that capability to conduct effective operations to counter threats to our national interests in cyberspace. Let me clear that we will only do so to defend our nation, to defend our interests, to defend our allies and we will only do so in a manner that is consistent with the policy principles and legal frameworks that the department follows for other domains including the law of armed conflict.

Which brings me to the second area of focus, policies and organization. Responding to the cyber threat requires the right policies and organizations across the federal government. For the past year, the Department of Defense has been working very closely with other agencies to understand where are the lines of responsibility when it comes to cyber defense. Where do we draw those lines? And how do those responsibilities get executed?

As part of that effort, the department is now finalizing the most comprehensive change to our rules of engagement in cyberspace in seven years. The new rules will make clear that the department has a responsibility, not only to defend DoD's networks, but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace. These new rules make the department more agile and provide us with the ability to confront major threats quickly.

To execute these responsibilities, we must have strong organization structures in place. Three years ago, the department took a major step forward by establishing the United States Cyber Command. Under the leadership of General Keith Alexander, a four-star officer who also serves as the director of the National Security Agency.

Cyber Command has matured into what I believe is a world-class organization. It has the capacity to conduct a full range of missions inside cyberspace. And it's also working to develop a common, real-time understanding of the threats in cyberspace. The threat picture could be quickly shared with DoD's geographic and functional combatant commanders, with DHS, with FBI and with other agencies in government. After all, we need to see an attack coming in order to defend against that attack.

And we're looking at ways to strengthen Cyber Command as well. We must ensure that hit has the resources, that it has the authorities, that it has the capabilities required to perform this growing mission. And it must also be able to react quickly to events unfolding in cyberspace and help fully integrate cyber into all of the department’s plans and activities.

And finally, the third area is to build stronger partnerships. As I've made clear, securing cyberspace is not the sole responsibility of the United States military or even the sole responsibility of the United States government. The private sector, government, military, our allies - all share the same global infrastructure and we all share the responsibility to protect it.

Therefore, we are deepening cooperation with our closest allies with the goal of sharing threat information, maximizing shared capabilities and determining malicious activities. The president, the vice president, Secretary of State and I have made cyber a major topic of discussion in nearly all of our bilateral meetings with foreign counterparts.

I recently met with our Chinese military counterparts just a few weeks ago. As I mentioned earlier, China is rapidly growing its cyber capabilities. In my visit to Beijing, I underscored the need to increase communication and transparency with each other so that we could avoid a misunderstanding or a miscalculation in cyberspace. This is in the interest of the United States, but it's also in the interest of China.

Ultimately, no one has a greater interest in cybersecurity than the businesses that depend on a safe, secure and resilient global, digital infrastructure. Particularly those who operate the critical networks that we must help defend. To defend those networks more effectively, we must share information between the government and the private sector about threats in cyberspace.

We've made real progress in sharing information with the private sector. But very frankly, we need Congress to act to ensure that this sharing is timely and comprehensive. Companies should be able to share specific threat information with the government, without the prospect of lawsuits hanging over their head. And a key principle must be to protect the fundamental liberties and privacy in cyberspace that we are all duty bound to uphold.

Information sharing alone is not sufficient. We've got to work with the business community to develop baseline standards for our most critical private-sector infrastructure, our power plants, our water treatment facilities, our gas pipelines. This would help ensure that companies take proactive measures to secure themselves against sophisticated threats, but also take common sense steps against basic threats. Although awareness is growing, the reality is that too few companies have invested in even basic cybersecurity.

The fact is that to fully provide the necessary protection in our democracy, cybersecurity legislation must be passed by the Congress. Without it, we are and we will be vulnerable. Congress must act and it must act now on a comprehensive bill such as the bipartisan Cybersecurity Act of 2012 co-sponsored by Senators Lieberman, Collins, Rockefeller and Feinstein.

This legislation has bipartisan support, but is victim to legislative and political gridlock like so much else in Washington. That frankly is unacceptable and it should be unacceptable not just to me, but to you and to anyone concerned with safeguarding our national security. While we wait for Congress to act, the administration is looking to enhance cybersecurity measures under existing authorities, by working with the private sector to promote best practices, increase information sharing.

They are considering issuing an Executive Order as one option to try to deal with the situation, but very frankly there is no substitute for comprehensive legislation and we need to move as far as we can in the meantime. We have no choice because the threat that we face, as I've said, is already here.

Congress has a responsibility to act and the President of the United States has constitutional responsibility to defend our country. I want to urge each of you to add your voice to those who support stronger cyber defenses for our country.

In closing, let me say something that I know the people of New York, along with all Americans, will appreciate. Before September 11, 2001, the warning signs were there. We weren't organized. We weren't ready and we suffered terribly for that lack of attention.

We cannot let that happen again. This is a pre-9/11 moment. The attackers are plotting. Our systems will never be impenetrable just like our physical defenses are not perfect, but more can be done to improve them. We need Congress and we need all of you to help in that effort. I want you to know the Department of Defense is doing our part.

And tonight, I'm asking you to do yours as citizens and as business leaders. Help us innovate. Help us increase the nation's cybersecurity by securing your own networks. Help us remain ahead of the threats that we confront. By doing so, you will help ensure that cyberspace continues to bring prosperity to your companies and to people across the world.

BENS has played an important part in this debate by identifying cybersecurity as a key national security challenge where business and government must partner together. And so I'd like thank BENS for your leadership in this area and thank you again for your recognition of the efforts that we have made. But more broadly, let me thank you for your commitment to the dream that guides all of us in this nation.

I talked about my parents as immigrants. And I used to ask my father why did he travel all of that distance to come to a strange land, leaving the comfort of family, it was a poor area in Italy, but why would you leave your comfort of family and travel all that distance to a strange land? And my father said the reason he did it is because he and my mother believed that they could give their children a better life. That is the American dream.

That's what we want for our children. We have achieved that dream because we always have been able to defend our interests and our values. That must remain our most important mission on land, at sea, in the air, in space and yes, in cyberspace. This is not just a responsibility, it is a duty that we owe to our children and their children in the in the future. Thank you very much.