

**SECRETARY OF DEFENSE LEON E. PANETTA**  
**“DEFENDING THE NATION FROM CYBER ATTACK”**  
**BUSINESS EXECUTIVES FOR NATIONAL SECURITY**  
**NEW YORK, NY**  
**THURSDAY, OCTOBER 11, 2012**

Let me begin by extending my deepest gratitude to Bruce Mosler and to BENS. Not only for this award, but for the important work that you do to foster an informed discussion about national security within the business community.

I'd also like to thank my friend Fran Townsend for serving as the Master of Ceremonies tonight. And, General Meigs, thank you for your leadership and for your distinguished service to this country.

I am honored to be with you all tonight.

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.

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've always been and always will be for the New York Yankees...unless they play the San Francisco Giants.

In all seriousness, I always appreciate the chance to come to this city – New York is a special place for me.

I've long appreciated New York's role as the center of gravity for our nation's economy. For that reason, it is an honor to be able to speak before this distinguished audience of business leaders and innovators. 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 at the very nexus of business and national security: the threats facing the United States in cyberspace, and the role the Defense Department must play in defending the nation from those threats.

This aircraft carrier is a fitting and appropriate venue to have this discussion.

This ship, and the technology on display at this museum, attest to one of the central achievements of the United States in the 20<sup>th</sup> century: our ability to project power and strength across land, the high seas, the skies, and outer space. Securing those domains helped ensure that they were used to advance peace and prosperity – not to promote war and aggression.

With that same goal in mind, today there is a new domain that we must secure to have peace and prosperity in the world of tomorrow.

Cyberspace has fundamentally transformed the global economy and our way of life, providing two billion people across the world with instant access to information, to communication, and to new economic opportunities.

Cyberspace is the new frontier – full of possibilities to help advance security and prosperity in the 21<sup>st</sup> century. Yet with these possibilities also come new perils. The Internet is open and highly accessible – as it should be. But that also presents a new terrain for warfare where adversaries can seek to do harm to our country, our economy and our citizens.

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

## AS PREPARED – EMBARGOED UNTIL DELIVERY

But the even greater danger facing us in cyberspace goes beyond crime and harassment. A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11. Such a destructive cyber terrorist attack could paralyze the nation.

Let me give you some examples of the kinds of attacks what 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 was unprecedented.

But even more alarming is an attack that happened two months ago, when a sophisticated virus called “Shamoon” infected computers at the Saudi Arabian state oil company, ARAMCO. Shamoon included a routine called a “wiper,” coded to self-execute. This routine replaced crucial system files with an image of a burning U.S. flag. It also put additional “garbage” data that overwrote all the real data on the machine. The more than 30,000 computers it infected were rendered useless, and had to be replaced.

Then just days after this incident, there was a similar attack on Ras Gas 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 this would have on your company.

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 the country.

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

Let me explain how this could unfold.

An aggressor nation or extremist group could gain control of critical switches and derail passenger trains, or trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country.

The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at once, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communications networks.

The collective result of these kinds of attacks could be “cyber Pearl Harbor”: an attack that would cause physical destruction and loss of life, paralyze and shock the nation, and create a profound new sense of vulnerability.

As Director of CIA and now Secretary of Defense, I have understood that cyber threats are every bit as real as more well-known threats like terrorism, nuclear weapons proliferation, and the turmoil in the Middle East. And the cyber threats facing this country are growing. With dramatic advances in cyber technology, potential aggressors are exploiting vulnerabilities in our security.

But the good news is that we are aware of this potential; our eyes are wide open to these threats; and we are a nation at the cutting edge of this new technology.

The Department of Defense, in large part through the capabilities of the National Security Agency, has developed the world’s most sophisticated system to detect cyber intruders or

attackers. And 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 investigating and preventing cyber attacks. And our intelligence agencies are focused on this potential threat. The State Department is forging an 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 one. Tonight I want to explain what that means.

But first, let me make clear what it does not mean. It does not mean the Defense Department will monitor citizen’s personal computers, or provide for the day-to-day security of private and commercial networks. That is not our mission.

Our mission is to defend this nation. We defend. We deter. And if called upon, we take decisive action. In the past, we have done so through operations on land and at sea, in the skies and in space. In this new 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 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 act.

To ensure we fulfill our role to defend the nation in cyberspace, the Department is focusing on three main tracks:

- (1) developing new capabilities;
- (2) putting in place the policies and organizations we need to execute our mission, and;
- (3) building more effective cooperation with industry and international partners.

### 1. Develop New Capabilities

DoD is investing more than \$3 billion annually in cybersecurity to retain cutting edge capabilities in this field. Following our new defense strategy, the Department is continuing to increase many key investments in cybersecurity even in an era of fiscal restraint.

Our most important investment is in the 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 operators.

We are recruiting, training, and retaining the best and 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 times per day. Through the innovative efforts of our cyber operators, we are enhancing the Department’s cyber defense programs. These systems rely on sensors and software to hunt down 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 we will be able to link them 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 an attack.

Over the last two years, the Department has made significant investments in forensics to address this problem of attribution, and we are seeing returns on those investments. Potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for actions that harm America or its interests.

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 or kill American citizens, we need to have the option to take action to defend the nation when directed by the President.

For these kinds of scenarios, the Department has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace.

Let me be clear that we will only do so to defend our nation, our interests, or our Allies. And we will only do so in a manner 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 our second area of focus.

## *2. Policies and Organizations*

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 closely with other agencies across the government to understand where the lines of responsibility in cyber defense will be drawn and how those responsibilities will be 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 will make the Department more agile and provide us with the ability to confront major threats quickly.

To execute these responsibilities, we must have strong organizational 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 a world-class organization.

Cyber Command has the capacity to conduct a full range of missions in cyberspace. It is also working to develop a common, real-time understanding of the threats in cyberspace. That threat picture could be quickly shared with DoD's geographic and functional combatant commands, with DHS and FBI, and other agencies in government. After all, we need to see an attack coming in order to defend against it.

We are looking at ways to strengthen Cyber Command. We must ensure that it has the resources, authorities, and capabilities required to perform this growing mission. 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.

### *3. Build Stronger Partnerships*

As I've made clear, securing cyberspace is not the responsibility of the United States military, or even the sole responsibility of the United States government.

The private sector, government, military, and 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 a goal of sharing threat information, maximizing shared capabilities, and deterring malicious activities.

The President, 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 – including with my 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 so that we can avoid misunderstanding or miscalculation in cyberspace. That is in the interest of the United States, and it is 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 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 have made real progress in sharing information with the private sector, but we need Congress to act to ensure 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, however, is not sufficient.

Working with the business community, we need to develop baseline standards for our most critical private-sector infrastructure – including power plants, water treatment facilities, and gas pipelines. This would help ensure that companies take proactive measures to secure themselves against sophisticated threats, but also take commonsense 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 Congress. Without it, we are vulnerable.

Congress must act, and it must act now on a comprehensive bill such as the bipartisan Cybersecurity Act of 2012, cosponsored by Senators Lieberman, Collins, Rockefeller, and Feinstein.

This legislation has bipartisan support, but it has fallen victim to legislative and political gridlock. That is unacceptable to me, and it should be unacceptable 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 cybersecurity best practices and increase information sharing. Issuing an Executive Order is one option under consideration.

There is no substitute for comprehensive legislation, but we need to move as far as we can in the meantime. We have no choice because the threat we face is already here. Congress has a responsibility to act. The President has a Constitutional responsibility to defend the

country. And 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.

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.

The Department of Defense is doing its part. 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 competition.

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. So I'd like to thank BENS members for your leadership in this area, and thank you again for this award.

But more broadly, let me thank all of you for your continued commitment to the dream that guides us as a nation.

It's the dream that brought my immigrant parents halfway around the world, through New York Harbor, to America. That dream is to give a better life for our children. We have achieved that dream because we have always 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.

Thank you.

###