

**The Honorable William J. Lynn III
Deputy Secretary of Defense**

Fletcher-IFPA-USAF Conference

“Aerospace and 21st Century National Security”

January 21, 2010

Thanks very much, Bob, for that kind introduction. This is quite a conference. A true master class in air, space and cyberspace issues. I can see by the number of people, the number of uniforms in the audience, I now have an explanation for why the halls of the Pentagon have been deserted the last day or so.

Before I turn to the topic of the conference, let me say a word about the operations in Haiti. The stories of our relief efforts emerging from Haiti should make us all proud. From the forward air controllers who started working from folding tables and chairs to bring order to air operations, to the Haitian-Americans serving in our armed forces who have found new uses for their native Creole language, to all the soldiers, sailors, airmen, marines and coast guardsmen working in difficult conditions to successfully deliver aid.

As of this morning, more than 13,000 U.S. service members are assisting the relief effort. About 10,000 on ships off-shore and about 3,000 ashore. These forces, together with their international counterparts and the government of Haiti are helping make a desperate situation a little less desperate each day.

As we speak, they're delivering 43,000 hand-held radios, working to reopen the port, and unloading cargo from more than 150 aircraft a day.

We are going to be there to see Haiti through to recovery, and as the President has made clear, we will render assistance as long as it is needed.

Let me now turn to the subject of today's conference. We meet at a time when the Air Force is making critical contributions on many fronts. To the mission in Haiti and other humanitarian efforts around the world, to our effort in Iraq and Afghanistan, and to the security challenges of tomorrow. So it's appropriate that we take two days to consider air, space, and cyberspace in the 21st Century. These three domains will be critical to our defense.

What I thought I'd do this morning is briefly share some thoughts on aerospace and space, but then I'd like to pivot and spend the bulk of my time talking about the newest domain, the cyber domain.

Our most important air and space mission is supporting our troops and those of our allies on the front lines. More than 100,000 of them wake up each morning in the Islamic Republic of Afghanistan. Tens of thousands more rise in Iraq. Our battlefield success in Afghanistan is to a

great degree underwritten by aviation and space platforms. In a land-locked nation with few workable roads, helicopter lift and cargo aircraft provide food, fuel and maneuver support. Combat air patrols and search and rescue teams watch over our troops day and night. Our offense against the Taliban and al-Qaida depends on air power. Because of a significant investment in intelligence, surveillance and reconnaissance, commanders receive actionable intelligence in minutes rather than hours. And unmanned aircraft now combine surveillance with new attack capabilities.

Many of these systems did not exist when the fight in Afghanistan began. Thanks to the leadership of Secretary Gates, we are making a major investment in their development, and we are surging those systems into theater. This is one area where lessons learned in combat are driving immediate institutional change and new budget priorities.

The Air Force for the first time has graduated more pilots of unmanned aerial vehicles than of fighters and bombers, and it's training more analysts to analyze video feeds from drones. The rapid fielding of unmanned aerial systems is one of many shifts we've taken across the department to focus our resources on the wars we are fighting and the new threats that we face.

This change has not come easily. Institutional change never does. But as President Obama has made clear, it's time to break out of "conventional thinking that has failed to keep pace with unconventional threats".

Of course the terrorist threat emanating from Afghanistan is not our only security challenge. The difficulty of this moment in time is succeeding where our troops are engaged without losing sight of the other threats we face and will face in the years to come.

The nature of war is changing in important ways. Conflicts are now of longer duration. Already we have been fighting in Afghanistan for longer than we fought in the 1st and 2nd World Wars combined. And our dominance in conventional warfare has led adversaries to seek new avenues to challenge us, particularly asymmetric and anti-access tactics.

Low end actors have access to high end capabilities. Insurgents wield IEDs that penetrate even the most heavily defended armor. Terrorists and rogue nations are seeking weapons of mass destruction.

In view of these changes, four overriding imperatives emerge in space and aerospace.

The first is to continue redirecting resources to defeat unconventional threats, including the full institutionalization of our ability to fight irregular wars. The second is the need to maintain our air superiority by investing in fourth and fifth generation tactical aircraft. No American ground soldier has been lost because of enemy air attacks since 1953. Although our strength in air and space far exceeds our competitors at present, the emergence of modern air defenses threaten the advantages that we have accrued.

Using readily available technology, potential adversaries are improving radars, sensors, jammers and weapons. To give our air and ground forces the freedom of movement that air superiority underwrites, we are heavily investing in the F-35. Indeed, a successful Joint Strike Fighter is at the heart of our continued air superiority. With more than 3,000 aircraft to be manufactured for us and for our allies, the Joint Strike Fighter represents a major investment in the future of air power.

This investment insures superiority against potential adversaries well into the foreseeable future. The U.S. is projected to have more than a thousand F-22s and F-35s before China fields its first fifth generation fighter.

Our third priority in aerospace is developing a next generation long-range strike capability. The ability to confront threats deep in enemy territory has always been a strategic priority for the Air Force. The long-range strike mission today is more fraught with challenges than it has been in memory. We're learning there is not a single solution to our needs, so we will be maturing a portfolio of capabilities—manned and unmanned, penetrating and standoff, ballistic and cruise. By working together, these new technologies will preserve our ability to swiftly and accurately confront threats to our security.

Our fourth priority is to ensure access to space and the use of our space-based assets. Space, much like cyberspace, is no longer a domain left uncontested by potential adversaries, so to protect our technological advantage in space-based platforms we must reduce their vulnerability to attack and to disruption.

The ability to rapidly augment our capabilities and to reconstitute them in the event of a successful attack will be a key tenet of our strategy going forward.

This balancing act between maintaining current programs and developing future capabilities is not easy to manage. And it is especially difficult in air and space, where decisions taken today will have consequences for how the force is equipped five, ten and fifteen years into the future. But we have to do it.

We have a Secretary who grasps this. He is committed to making the difficult judgments that are needed. This was evident in the FY10 budget, and it will be equally true in the FY11 budget that we'll release next week.

Our criteria for exercising program discipline are clear. Programs that are performing poorly--either over budget, behind schedule, or delivering less capability than promised--open themselves up to reconsideration.

Programs that offer admittedly elegant capabilities, but at too high a price or in too small of a niche area, are also ripe for reshaping. And programs that provide capabilities we already have enough of will be supplanted by others that help us meet new threats in new ways.

The bottom line is that by exercising program discipline we're becoming a better and more capable department.

In the aggregate, these tough decisions enhance our ability to protect the American people. In the heat of the budget debate, we must never lose sight of that bigger picture.

In that bigger picture, one threat has particularly captured my attention. I'm often asked what keeps me up at night. Number one the cyber threat. If we don't maintain our capabilities to defend our networks in the face of an attack, the consequences for our military and indeed for our whole national security could be dire.

To give you a sense of how difficult cyber attacks can be, I want to take us through one actual cyber intrusion. This particular incident started when warning flags appeared on Air Force computers. Unauthorized activity was detected at Andrews Air Force Base and soon thereafter in half a dozen networks across the country. The attacks were coordinated and aimed at crucial military systems. The threat was so serious that the President was briefed. Investigators at first had no idea where the attack was coming from, but soon they discovered a cyber trail that stretched halfway around the world to compromised computers on three continents. Eventually they traced the origin of the attack to a commercial service provider in California and a server in the Middle East. The attackers were exploiting a vulnerability in the Unix operating system. The security flaw was known, but defensive measures had not yet been put in place. This left unguarded a back door to DoD's computers.

The good news is our law enforcement agencies and intelligence services stopped the attack within a week. The instigators turned out to be two teenaged hackers from California who had the help of an experienced cyber criminal. They were arrested and tried on charges of computer assault. Some of those in this room helped solve this incident, which came known as Solar Sunrise.

The bad news is that this intrusion happened in 1998 and it's child's play compared to what's happening today. Over the past ten years the frequency and sophistication of attacks have increased exponentially. Our networks are under threat every hour of every day. They are probed thousands of times a day. They are scanned millions of time a day. And we have not always been so successful in stopping intrusions or determining where they come from.

Cyber is an especially asymmetric technology. The low cost of computing devices means that our adversaries don't have to build an expensive weapon system, like a fifth generation fighter, to pose a disproportionate threat. Knowing this, many militaries are developing offensive cyber capabilities, and more than 100 foreign intelligence organizations are trying to break into

U.S. systems. Some governments already have the capacity to disrupt elements of the U.S. information infrastructure.

We recently caught a glimpse of what cyber war might look like. When Russian tanks rumbled into Georgia, cyber attacks simultaneously crippled Georgian web sites.

But cyber attacks are not limited to the battlefield. Organized criminal groups and individual hackers are building global networks of compromised computers. These BotNets are becoming instruments of cyber crime. Our financial system and our critical infrastructure are at risk. Sustained power outages and breakdowns in our transportation system could lead to physical damage and economic disruption.

Nor are our networks impervious to espionage and theft of our commercial information, as Google and 33 other companies discovered last week. The Library of Congress holds more scholarly material than has ever been brought together in all of history, yet an amount of intellectual property many times larger is being stolen each year from networks maintained by U.S. businesses, universities and government agencies.

Not even the President has been spared. During the presidential campaign in 2008, hackers gained access to campaign files of both Barack Obama and John McCain. Policy papers, travel plans, and sensitive emails were all compromised. The intrusion was eventually detected and repelled, but not before sensitive information was taken.

For all these reasons the President has called the cyber threat one of the “most serious economic and national security challenges we face as a nation.”

Because of the seriousness of this threat, the Defense Department has formally recognized cyberspace for what it is — a domain similar to land, sea, air and space. A domain that we depend upon and must protect.

It’s the only one of the domains that is manmade, but it’s just as critical as the others. Just as our economy and our national security depend upon freedom of navigation of the seas, they also require freedom of movement on-line.

Over the past ten years we have built layered and robust cyber defenses. We began by developing the capability to detect and mitigate cyber intrusions. To spearhead our efforts we stood up the Joint Task Force Global Network Operations, an arm of STRATCOM co-located at the Defense Information Systems Agency, and we also stood up the Joint Functional Component Command Network Warfare, another arm of STRATCOM co-located with the National Security Agency. The former defended our global military networks; the latter applied NSA capabilities on signal intelligence and information assurance to address cyber threats.

Through these efforts new capabilities to secure our networks gradually came on-line. We deployed host-based security services, intrusion detection systems, network mapping and visualization software which helped us hunt on our own networks.

Our defenses need to be dynamic. A fortress mentality will not work in cyber. We cannot retreat behind a Maginot line of firewalls. Cyber war is much more like maneuver warfare, and these new technologies help us find and neutralize intrusions. But we must also keep maneuvering. If we stand still for a minute our adversaries will overtake us.

The task is enormous. All told, our department operates 15,000 networks across 4,000 installations in 88 countries. We use more than 7 million computer devices. It takes 90,000 personnel and billions of dollars annually to administer, monitor and defend those networks. And yet the cyber threat continues to grow.

To combat it we need the military and intelligence community to unify their efforts. At present, military cyber capabilities are spread too far and too wide, both geographically and institutionally, to be completely effective. The scale of the enterprise has outgrown current structures, placing our cyber advantage at risk.

To ensure our network administrators can support our operational needs, we must pull together the activities of our military services. We need more than a patchwork quilt of joint task forces and functional components. We need the level of resources, stature and global reach that a four-star command can bring. We need to institutionalize what has been ad hoc, continually evolving solutions that build off each other but never quite become greater than the sum of their parts.

In June, Secretary Gates approved a new Cyber Command as a sub-unified command of STRATCOM. Cyber Command will be based at Fort Meade where it will benefit from the tremendous expertise of the National Security Agency. The President has nominated NSA Director Lieutenant General Keith Alexander to head the command, thereby combining the leadership for NSA and Cyber Command into one dual-hatted position.

Cyber Command will bring together more than half a dozen intelligence and military organizations in support of three overlapping categories of cyber operations.

First, CYBERCOM will lead the day to day defense and protection of all DoD networks, raising our situational awareness and control.

Second, CYBERCOM will coordinate all DoD network operations providing full spectrum support to military and counter-terrorism missions.

Third, CYBERCOM will stand by to support civil authorities and industry partners on an as-needed basis.

Combining offensive and defensive capabilities under a single roof and bringing those together with the intelligence we need to anticipate attacks will make our cyber operations more effective. This linkage among offense, defense and intelligence is particularly important in cyber because the capability to repel attackers is closely tied to the ability to identify threats and anticipate intrusions.

CYBERCOM will also help develop threat conditions that calibrate our defenses in peacetime, crises, and war. Like the DEFCON system that we have for nuclear war, CYBERCON levels will help us determine when we raise and lower our defenses.

At the same time, each service will have a component command working in support of CYBERCOM. The Army's Network Enterprise Technology Command in Arizona; the Navy's 10th Fleet Cyber Command; and the 24th Air Force will all supply personnel to CYBERCOM and help implement its directives across the force.

While CYBERCOM ensures that our capabilities and force structures are aligned with the National Military Strategy and coordinated with other government agencies, the component commands will make cyber a regular part of training and equipping the force. And to ensure all DoD cyber operations are unified under a single leader, a chain of command with clear legal lines will run from CYBERCOM to units around the world.

With CYBERCOM the progress we are now making is significant. However, there are still areas in which we need to take action. The challenges ahead in many ways are as conceptual as they are technical. For example, we need to examine how concepts of deterrence apply to the cyber domain.

Nuclear deterrence has always relied on identifying attackers. This is not a problem with missiles. They come effectively with a return address. But in the cyber world it's often very difficult to identify the origin of an attack. Even if it is identified quickly, cyber attackers may not have assets that we can strike back at. Shutting down a server that's stolen from someone who's not even witting of it is not an effective deterrent. For these reasons the Cold War model of nuclear deterrence does not wholly apply to cyber.

But there are continuities with established paradigms of deterrence and defense. For instance, we can enhance our defenses by working with our allies. International cooperation is imperative for establishing the chain of events to an intrusion. In this way the construct of shared warning applies to cyberspace. Just as our air defenses are linked with those of our allies to provide warning of an airborne attack, so too can we cooperatively monitor our computer networks.

This year I will be working to deep our cyber cooperation with many of our allies.

The internet has turned the world into a digital community. Each member now has a role in keeping the neighborhood safe. But working with other nations raises still more questions about how cyber attacks affect the legal framework for conflict.

For instance, what role does sovereignty play when computer networks cross multiple borders? How do we distinguish between a hacker's exploits, criminal activity, espionage, and an attack on the nation? When exactly is a cyber attack an act of war? What kind of response to an attack is appropriate, proportional and justified? And defending against cyber threats is made even more complex by the fact that the cyber domain is largely owned by private entities.

We are starting to get our arms around how we organize the government to assist the private sector. Doing so will require overcoming a mismatch of capabilities and authorities. The Department of Homeland Security appropriately has the lead to protect the dot-gov world, but ten years of concerted investment on the military side has placed much of our cyber defense capabilities within DoD and the intelligence agencies. So at present, using government tools to protect private sector networks and the dot-gov networks entails cross-agency collaboration. How we align agency capabilities with our national cyber objectives is a difficult problem and it's not yet been fully solved.

Using government tools to protect private networks also raises difficult practical questions. Making networks safer will ultimately require pushing down software that can detect patterns of threatening activity to a large number of users, but attack vectors and signatures of cyber threats are often classified.

We need to think imaginatively about how government technologies can help secure a space on the internet for critical commercial and infrastructure applications. For example, could we create a secure architecture for the dot-com world that lets private parties opt in to government protection?

How the private sector will organize itself to defend against the cyber threat is also unresolved. Existing technologies can thwart a majority of cyber attacks, but defenses are expensive and burdensome. Although many industries have made a major investment in defensive capabilities, not everyone is able to make that kind of investment. How do we put in place the appropriate incentives to motivate private investment in cyber defenses?

So in the cyber domain we face enormous foundational challenges. We must not only develop a military doctrine for protecting our networks, we must also decide how our government as a whole will leverage its capabilities to defend our country and our economy.

At DoD we're working hard on the doctrinal issues and on developing the capacity to thwart attacks, but much of this effort requires collaboration with other parts of the government, with the private sector, and with our allies.

We're working closely with the White House and the Department of Homeland Security to work through these issues. The White House has just named Howard Schmidt as the White House Cyber Coordinator and he will be leading the National Security Council's effort to organize the government's cyber activities.

As you can see, I have a lot to think about when I wake up at night, but all of us do.

Although the challenges we face in cyber seem daunting, it is useful to remember that with cyber we are only at the beginning of a new technological age. At this early hour our greatest strength is our awareness of the transformation happening around us. Our predicament calls to mind a letter urgently written to President Roosevelt on the eve of another technological effort. On August 2, 1939, he received a letter that said, "Aspects of the situation which has arisen seem to call for watchfulness, and if necessary quick action on the part of the administration. I believe, therefore, that it is my duty to bring to your attention the following facts...and to put forward recommendation for government action."

The letter was signed, "Yours Truly, Albert Einstein." It was Einstein's warning to Roosevelt that breakthroughs in nuclear fission might make possible an atomic bomb.

The letter led Roosevelt to launch the Manhattan Project, which ultimately helped end a world war.

The cyber threat does not have the existential implications ushered in by the nuclear age, but there are some important similarities. In the military arena, cyber attacks offer a means for potential adversaries to overcome our overwhelming advantages in conventional military operations. Perhaps more strikingly, cyber attacks pose a serious danger to critical aspects of our civilian infrastructure. They may not cause the mass casualties of a nuclear strike, but cyber attacks could wreak havoc on our financial system, our power grid, and our transportation network. And over time the systematic penetration of our universities and businesses could rob us of maybe our most significant source of strength, our intellectual property.

It is now upon us to devise an effective defense before our adversaries act further against us. We must make the cyber domain safe so that revolutionary innovations can be used without fear of endangering our national security.

With that, I'm happy to take your questions.

###