Center for Strategic and International Studies (CSIS)

Global Security Forum 2011 Keynote Address

Welcome:
John Hamre,
President & CEO,
CSIS

Speakers:
Simone Bemporad,
CEO,
Finnmeccanica North America, Inc.

William J. Lynn, III,
Deputy Secretary of Defense,
U.S. Department of Defense

Washington, D.C.
Wednesday, June 8, 2011
8:00 A.M.

Transcript by
Federal News Service
Washington, D.C.

JOHN HAMRE: Ladies and gentlemen. (Pause.) Well, you quiet down real good. (Chuckles.) Thank you all very much for coming. We're delighted to have you here. Welcome to the Global Security – the Global Strategy Forum 2011 (sic). We are very pleased to have you. It's going to be quite an interesting day. I must say, there's enough of me to clone but unfortunately, I can't get cloned. I would like to attend almost all of the seminars that we have today, and I'm sorry we're not going to let everybody attend everything, but we just had too much to do and too little time. And so we're very anxious to have all of you here and welcome. We're delighted you're with us.

I would like to say a special – first of all, I can't thank all of the people from the podium who have been instrumental in this. We've got dozens of speakers who have been willing to give their time and participate and my remarkable staff. Gosh, I love this staff. They're just fabulous – have been working so hard for months, now. And it's going to be a great day and I'll thank all of them in a very special way later but wanted to acknowledge this contribution that they've done today.

I also would like to say just a very sincere word of thanks to our friends at Finnmeccanica. Finnmeccanica has made this possible – for us to be able to host this. This is the second year. And I would like to invite Simone Bemporad to come to the podium and briefly say some words of welcome on behalf of Finnmeccanica. (Applause.)

SIMONE BEMPORAD: Thank you. Good morning, ladies and gentlemen. Thank you, John, for your kind introduction and for keeping us, today, under the air conditioning because it's going to be 95, 97 (degrees Fahrenheit) today.

I would like to welcome you to today's event and extend to each of you the regards of our chairman, the Finnmeccanica chairman, Pier Francesco Guarguaglini and our CEO, Giuseppe Orsi, and the Finnmeccanica senior defense advisory committee who are in the audience this morning. I would also like to recognize, of course, today's keynote speaker, the Honorable Bill Lynn, deputy secretary of defense, and all the other esteemed panelists.

Finnmeccanica is proud to support the mission and activities of CSIS. Under the leadership of John and his team, CSIS has become one of the best-regarded organizations in global security issues. We at Finnmeccanica understand the importance of contributing to groups like CSIS and to fostering objective analyses of key policy issues.

Today's global security forum panelists are leading experts in their fields. The fact that CSIS can attract this level of talent is a testament to its reputation of commitment to excellence. Finnmeccanica shares the same commitment to excellence, a value that is realized daily by our 12,000 American employees and by another 63,000 around the world. We are dedicated to delivering the best products and services to our customers and to supporting the servicemen and women around the world.

Thank you again for being part of this special day. I hope and I'm sure that you will find this forum productive and interesting. Thanks. Thank you, John. (Applause.)

MR. HAMRE: It's my great pleasure now to introduce Bill Lynn. Bill and I – we go back quite a few years – actually, over 30 years. We first started working together back up in the Senate. At the time, I was on the Armed Services Committee and Secretary Lynn was working, at that time, for the late senator Ted Kennedy.

And we became fast friends and our trajectories in life have interwoven since that time when, during the Clinton administration, Secretary Lynn was, at that time, the director of program analysis and evaluation, initially, and then became the comptroller. And so we've had – you know, that was before he became a virgin, I mean, his comptroller thing. And so we've had a remarkable experience in life of having get to know each other.

Before that, and before I really knew Bill, he was actually at CSIS. We did a landmark study in the 1980s that led to Goldwater-Nichols, and it was the intellectual foundation of Goldwater-Nichols. And Bill, along with Barry Blechman, were the two lead investigators that made that work possible.

So when I called the secretary and said we would like to have him keynote a speech today, he said, what do you want me to talk about? I said, anything you want. Well, I didn't anticipate the future of war to be the topic, but I'm looking forward to this more than anybody. So would you please join me in welcoming Secretary Bill Lynn? (Applause.)

WILLIAM J. LYNN, III: Thanks very much, John. It's a pleasure to be with you here today and great to see how many people get up this early. I thought it was just the Pentagon. The past decade has been filled with enormous changes and challenges in national security. And there have been few constants, but one of the constants has been the leadership that John has provided here at CSIS.

He's made CSIS firmly at the pinnacle of the think tanks here in Washington, making enormous contributions to the debates, both in terms of the substance of the debates, as well as bringing people of disparate views together and trying to find common ground. And John is now just at the point, now, of finding new ground for CSIS. He tells me that not next year at this time, but the year after, we will be at the new building that John's raised the capital for and will have just broke ground on, I think, just in the last –

MR. HAMRE: We still need contributions.

MR. LYNN: Yeah. (Laughter.) We'll have an offering later in the talk. (Laughter.) I do have, though, one complaint for John. As he said, we do go way, way back and, given our friendship, I would have thought he would have warned me about this job – that it turns out that, well, he's now the CEO of CSIS, which means he has a deputy. He is no longer a deputy.

And what it turns out and John didn't tell me is that deputy is the worst job in Washington. (Laughter.) What happens is, all of the issues that have solutions that please large constituencies and make everyone happy are picked off underneath you. An undersecretary of defense makes a decision, issues a press release, takes credit. Everybody's happy, except, of course, me. (Laughter.)

It's only the really intractable issues that move their way to my office. And then once in a while, a sexy issue will make its way through this maze and get there, at which point, Secretary Gates reaches down, grabs that one, says, don't worry about that, big guy. I have it. You don't need to go any further on it. So except for that one point, John, it's been a fabulous 30 years.

What I'd like to do is, as I said, John, is talk – I hope it's not as grandiose as the title suggests – but I'd like to talk about some of the concerns that we have as we think about the future of war. And we have to think about it in the fact that, since 9/11, for the decade after 9/11, we've had the ability to address new defense challenges by simply increasing the amount of resources we put against defense.

And it's clear, however the debate on deficit reduction and the national debt come out, we're not going to have that luxury for the foreseeable future. It's clear that the deficit crisis requires all of our government functions to reduce their planned spending levels, and defense will be no exception. It's not plausible, programmatically or politically, to exclude the 20 percent of government spending that's encompassed by the defense function from deficit reduction plans.

So the challenge we face today is to manage the coming slowdown in defense spending wisely and responsibly. This requires making judgments about the nature of our future security environment, which is an exceptionally tricky business. As that great strategist, Yogi Berra, said, predictions are difficult, especially about the future. In fact, we have a poor track record of projecting when, where and against whom we will fight.

Secretary Gates has described our record in that regard as perfect: We have never gotten it right. But there is one area where I'd argue our predictions have a better record, and that is with regard to the future of war itself – that is, how wars will be fought, what technologies will be transformative and what tactics will be effective.

Nations that have accurately predicted prior trends in warfare emphasized maneuver warfare over fortifications, bought aircraft carriers instead of battleships and understood the paradigm-shifting nature of nuclear weapons. In order to sustain the right defense capabilities in the coming spending slowdown, we need a similarly considered understanding of future strategic trends.

For most of human history, we've fought our battles on land and at sea. It's only been in the last century that the terrain of war has spilled into the air and under the ocean. And space first figured in conflicts less than three generations ago. Most recently, we find ourselves operating in and depending on cyberspace. So warfare, first transformed by the Industrial Revolution, then by the atomic revolution, is now being revolutionized by the information age.

This is the national security environment of the 21st century: diverse military actors and capabilities acting simultaneously across multiple domains with more interdependencies than ever before. The full scope of this extraordinary transformation was witnessed by a man we paid tribute to earlier this spring. Frank Buckles was 110 years old when he passed away in February. He was the last surviving U.S. veteran of the First World War, of the nearly 5 million who served.

The story of his life and how warfare changed during it gives us insight about our future strategic environment. Born in a barn by lantern-light, Buckles bluffed his way into the Army at the age of 16. Weeks after enlisting, he set sail on the ocean liner *Carpathia*, the same ship that rescued the Titanic survivors. In France, Buckles saw the horrors of trench warfare firsthand while serving as an ambulance driver on the Western Front.

The tide of history swept over Buckles again in 1941, when the Japanese invaded the Philippines, where he was working as a shipping merchant. He was held prisoner for 38 months until the Army rescued him and his fellow prisoners in a daring parachute raid behind enemy lines. The very week he was rescued, the design for the atomic bomb was finalized, ushering in a new era of warfare that eclipsed industrial might alone.

Buckles went on to farm cattle in West Virginia. There, he rode his tractor until well after the age of 100. Even at that age, he participated in the next great transformative revolution, the introduction of the information age. Buckles, as his obituary noted, was one of the few Americans born in the McKinley administration to have a Facebook page. (Laughter.)

The three revolutions that Buckles' life encompassed brought an avalanche of military technologies and introduced whole new dimensions to war. The implications of these past shifts for the military have been profound. The issue for us to consider today is what capabilities and what programs to protect in a defense drawdown and what course future technological trends will take.

In that context, I would identify three strategic trends that could shape our future national security environment: lethality, duration and asymmetry. Each of these trends has implications for how we design our defense programs going forward. Each, if not carefully managed, could weaken our security. The first and most prominent trend in the global strategic environment has to do with access to lethality.

Previously, when you looked at the range of threats we faced, the more capable the potential adversary, the higher the level of lethality they possessed. For centuries, the most economically developed nations wielded the most lethal military power. Secondary actors on the international stage possessed second-rate capabilities. Developing countries and insurgent groups had little access to highly lethal technologies.

Today, that linear relationship between economic power and military power no longer holds. Terrorist groups with few resources can mount devastating attacks. Insurgents can defeat our most advanced armor with fertilizer bombs. Rogue states are seeking nuclear weapons, and

even some criminal organizations now possess world-class cyber capabilities. The three revolutions that Frank Buckles lived through have granted low-end actors access to high-end capabilities. Lethality at the low end of the spectrum can now rival that at the high end.

As a result, the most sophisticated and unconventional opponents pose credible challenges to our security. The change in lethality has increased the risks we face and diversified the range of threats that we must be prepared to confront. Defense planning must reflect this development. Our military must be able to confront both high-end and low-end threats. We must have what Secretary Gates called a portfolio of capabilities with maximum possible versatility across the widest spectrum of conflict.

The increase in lethality across the threat spectrum means we cannot prepare exclusively for either a high-end conflict with a potential near-peer competitor or a lower-end conflict with a counterinsurgency focus. Because our ability to project force is challenged by either scenario, we must maintain capabilities to meet both. We do have decisions about how to size our forces for these disparate contingencies, but we must equip for both.

In other words, we will need both fifth-generation fighters and counter-IED technology, going forward. This increase in lethality also has implications for homeland defense. For a century, before World War II, our oceans insulated us from attack. Even after the advent of the nuclear age, only a nuclear-armed superpower could truly threaten our homeland.

But now technology allows small groups with focused lethality to wield influence that only nation-states could wield before. The increase in lethality, whether due to weapons of mass destruction, cyber attacks or IEDs, has changed forever the relationship between homeland defense and national security.

The second strategic trend is the increasing duration of warfare. For several decades of military planning, we have assumed kinetic engagements would be relatively short, and that is how we plan – for intense, but ultimately short battles that yield a decisive victory. Desert Storm has been the prototype – a month-long aerial bombardment and a hundred-hour ground campaign with clear transitions between conflict and post-conflict phases.

This construct does not fit with our current reality. For most of the past decade, we have been fighting two wars. Each began with an intense combat phase, but then as the adversary persisted, the transition between conflict and post-conflict became unclear and the scope of our mission expanded dramatically. Our deployments to Iraq and Afghanistan have now lasted longer than the U.S. participation in World War I and World War II combined.

The stress this places on our force turns out to be far more challenging to manage than the intensity of the initial kinetic phase. A central concern, then, for the department is managing the burden the duration of conflict places on our troops, their families and the national treasury. This trend, too, has important implications for force planning. We must plan for sustained, long-term commitments for a range of plausible conflicts.

Because duration becomes as important a driver of planning as intensity, we must maintain enough force structure to allow adequate dwell times between deployments. This is likely to have important implications for how we size, structure and utilize our reserve-force components. We need the ability to scale up force structure for longer conflicts, and the long-term conflicts must be considered in our strategic calculus.

The third and final trend in war is the increasing prevalence of asymmetric threats. Battlegrounds used to be a meeting place of like-on-like forces: cavalry on cavalry, armor on armor and, in the Cold War, nuclear against nuclear. We generally faced enemies whose framework for the use of force was similar to our own. Our challenge was to develop superior capabilities and tactics within that framework.

This like-on-like paradigm is disappearing. In stature, the American military is dominant by almost any measure. There are very few militaries that can or will challenge us directly. Yet, we are finding that very dominance causes our adversaries to become more creative in their approach. Today, adversaries can defeat us only if they sidestep our construct for the use of force. Our adversaries depend on asymmetric approaches that target our weaknesses and undercut our advantages.

So insurgents such as the Taliban and al-Qaida in Iraq avoid engaging our military in direct, force-on-force engagements. Instead, they use IEDs and assassination as their weapons and they hope to use the longer duration of war to wait us out. But unconventional forces are not the only ones to embrace this asymmetric approach. Traditional powers are seeking asymmetric capabilities.

Anti-access and area-denial strategies are perhaps the most vivid example of this approach in conventional conflict. Rather than confront our substantial conventional advantages in power projection at sea and in space, some nations are pursuing ballistic missiles that seek to push our forces further from the battlefield. In this way, asymmetric tactics are being built directly into conventional capabilities our forces may face in the future.

The source of the area-denial and anti-access tactics is the proliferation of precision-strike munitions. From Desert Storm to the present, the United States and its allies have had relatively exclusive access to these sophisticated, precision-guided munitions. Over the next decade or two, though, that technology will be increasingly possessed by a range of other nations. The diffusion of precision-strike technology will have a cumulative effect.

It will enable anti-access and area-denial strategies, thereby creating challenges for our ability to project power to distant parts of the globe. To address these challenges, we need to develop a range of capabilities, particularly missile defense and long-range strike. The ability to strike targets worldwide is an important deterrent against aggression, so we're making a major investment in a family of long-range strike systems that will allow us to penetrate defenses and deliver munitions worldwide.

This family of systems includes electronic attack capabilities, more advanced intelligence and surveillance platforms and ultimately, a new long-range bomber capable of both manned and

unmanned operations. Asymmetric tactics are also spreading beyond the traditional domains. Potential attacks in cyberspace perhaps best illustrate the growing asymmetry in warfare. Internet technology increasingly underpins both our military and economic strength, but in turn, this reliance on information technology has created new vulnerabilities.

Those wishing to cause us harm no longer need an industrial complex to marshal deadly force. Advanced weapons systems like a fifth-generation fighter or a carrier battle group require major investments in research, development, production and a significant technological base. In contrast, cyber capabilities have lower barriers to entry.

A small number of highly trained programmers, using off-the-shelf equipment, can develop quite destructive tools and deploy them to great effect. This cyber threat is maturing in two dimensions. To date, we have primarily seen cyber tools that have been used to exploit information or to disrupt networks. We are only beginning to see cyber tools that can be used to cause physical effects, but tools that can cause physical destruction are out there.

The cyber threat is also intensifying in a second dimension. Presently, the highest levels of cyber capabilities reside primarily with nation-states. But because our military power provides a strong deterrent, most nation-states have no more interest in conducting a destructive cyber attack against us than they do in conducting a conventional military attack. The risk for them is too great. So even though nation-states are the most capable actors, they are the least likely to initiate a destructive attack, at least in current circumstances.

Terrorist groups, however, have no such hesitation. With few assets to strike back at, they are harder or impossible to deter. If a terrorist group gains a disruptive or a destructive cyber capability, we have to assume they will strike with little hesitation. So in cyber, we have a window of opportunity to act before the most malicious actors acquire the most destructive technologies.

We need to continue moving aggressively to protect all of our critical networks – our military networks, our government networks and the networks that support our critical infrastructure. The bottom line is that in the cyber arena, as well as the other asymmetric threats – all require us not to become complacent with our conventional military superiority.

Just as World War I showed the obsolescence of cavalry and World War II, the battleship, we may be surprised at how rapidly our current, state-of-the-art systems are overcome by developments that we cannot foresee today. Let me conclude by saying that, in predicting the procedure, I proceed cautiously. I don't have a crystal ball. I do agree with Yogi Berra.

But I also believe that we can make informed judgments about the future of war by looking beyond specific scenarios to the underlying trends of warfare and the historical forces that drive them. The three trends that I have just described – the increasing access to lethality across the threat spectrum, the longer duration of warfare and the growing prevalence of asymmetric threats – pose challenges to our projection of power.

They are each, in different ways, the result of our entry into a new era of warfare – one driven primarily by the overlay of the information age atop the industrial and atomic revolutions. They can and must inform our defense planning. What we need to do, at this juncture in this fiscal environment, is to take the long view about what strategic trends are important, which brings us back to Frank Buckles.

In his lifetime, he saw firsthand the impact of the industrial age on warfare in World War I. He witnessed the dawning of the atomic age during and after World War II, and he lived to be a participant in the information age. The 16-year-old farmboy who fought in the first World War and survived the second to see the impact of each of these revolutions in warfare. During this same period, Frank Buckles also witnessed an extraordinary series of U.S. military innovations, from biplanes to UAVs, from machineguns to precision-guided weapons, from telegraphs to satellites.

Buckles watched these innovations help our forces maintain and expand their edge over our adversaries. Now the challenge for us is to navigate our nation's fiscal circumstances without disrupting the capabilities of the world's most effective fighting force. We need to make the right judgments about the nature of our future security environment.

We need to invest in the right capabilities and force structure that address trends in warfare that I have just outlined. And we need to relentlessly adapt our technology and our doctrine as threats evolve and mature. If we are able to do these things, we'll ensure our forces are ready for the future of war. Thank you. (Applause.)

MR. HAMRE: We have microphones that are around the room, and we'll take questions. And so please indicate – the secretary is going to field them himself – but identify who you are, please. We've got a –

MR. LYNN: I'll pass the hard ones to John. (Laughter.)

MR. HAMRE: We need somebody down in the front.

Q: Good morning. Thank you for your comments. My name is Paula Stern, and I came to hear about the future of war, but I came away from your comments to ask you on behalf of one of my clients, which is the National Center for Women and Information Technology, to address the personnel issue in the information age.

You emphasized, particularly in your third trend, this increasingly important trend regarding America's preparation for the future in defending of our nation. Can you address, please, the ability to access, in our citizenry, the adequate numbers and quality and diverse thinking for the information age?

Specifically, we had the national foreign defense language fellowships, years ago, when it came to the Soviet Union. Do we need something like that from Department of Defense to ensure that we have the adequate capability, in numbers and in quality and diversity of thinking, to design those forces that you described?

MR. LYNN: Well, going back to just the kind of historical sweep, I think the implication of your question is right, is that as we've moved through each of these revolutions in military and industrial affairs, the importance of trained people has grown. When you moved from the industrial age to the atomic age, it grew; when you moved from the atomic age to the information age, it's grown still farther. And I think, indeed, it doesn't go too far to say that our qualitative edge that our military enjoys today is largely due to the quality of our people. Our equipment is great, too, but at the end of the day, if you don't have the trained people to operate it, it won't be effective. Going to, more precisely, your question, I do think we need to focus on, how do we make sure that we are able to continue to bring the right trained people in, or the people trained in the right fields, into our military. And cyber is certainly a critical one. The Cyber Command, National Security Agency, the Homeland Security Department, other agencies are very much focused on that. At DOD, we've set up exchanges with industry. We're looking at innovative programs with the National Guard and Reserve where we might be able to utilize people who – where their day job is in the information technology industry, we might try and bring them into that field, specifically, in DOD, rather than just a more general recruiting. So we need to look at that. And then finally, I'd say a role that DOD, I think, can play more generally – broader than just people and training – in cybersecurity, I think, is similar to the role DOD played with high-performance computing. There are important defense needs for high-performance computing but it obviously has much broader societal impacts, and what DOD was able to do was seed some of the research and accelerate some of the research. And I think in cyber, it could be the same. It will be a fraction of the research and R&D, but I think if we focus it appropriately, we can help accelerate and maintain our competitive edge in this critical field. Sir – now we have to find a microphone.

Q: Hi, I'm Hank Gaffney from CNA. I hear, as you speak about all this future warfare and warfare all over the world and all these adversaries, nobody ever specifies those adversaries. They're quite finite, actually. Plus the fact that two-state wars have just about disappeared, as you said – conventional wars – internal wars are going down at a very rapid rate, as shown by all the studies.

So it sounds like there's a lot of exaggeration here because, when you come down to it, what have you got? North Korea, which is collapsing and starving; China, which is embedded in the world economy; Iran; Hezbollah, which some have described as the biggest threat since the Soviet Union; and, of course, a big problem in Mexico; and of course, the terrorists, who are wildly dispersed at this moment. How do you corral in all the work you do within defense to avoid exaggerations and be more specific about the situations, adversaries that we have to face?

MR. LYNN: Well, I think the thrust of my remarks went in the opposite direction of where you're going. I think that our ability to predict, in the way you're trying to do, has shown itself to be a failure, time and time again. The statements that you just made could have been made a decade ago. You would have said, well, China has problems. North Korea is the principal threat but they're starving. And then we went on and fought in Iraq and Afghanistan without anticipating them. As Secretary Gates said, we have a perfect record. If you look, I'd say, a year out from most of the conflicts that we've gotten involved in – there may be one or two exceptions – you would have had no idea we were going to be in them a year before they

happened. So I think it's a very difficult proposition to try and do your defense planning based on specific scenarios that you outlined. I think that what you have to do is more along the lines of what I've said. You have to assess what kind of capabilities do you think we might need, what kind of threats might we face if the conflicts appear and how do we develop capabilities to counter those threats. I don't see your alternative, really, as workable.

Q: Thank you, Mr. Secretary. Don Loren from the Tauri Group. Thank you for joining us this morning. Thank you for your years of service to the nation. I think your analysis is excellent. The trends are right on the mark. Good comments.

There are many obstacles to executing a plan to address those trends, and two that jump out are an extremely burdensome and bureaucratic acquisition process that could take as long as 15 years from concept development to actually producing a piece of kit and getting it out there for use by our forces – many milestones along the way, lots of decisions, lots of influence from Capitol Hill, many, many factors that require us to take excessive amounts of time to produce pieces of kit.

The second, I think, would also be funding with respect to R&D and rapid fielding for the type of equipment, the type of counter-strategies that are required to address your trends. So what do you see on the horizon for the Department of Defense to address those two major obstacles to executing a strategy to plan against your trends?

MR. LYNN: I mean, I agree with your description of the obstacles and the difficulties of the acquisition process, and we are trying to address those. We're trying to, in particular, break out the information technology world as different, in terms of how you ought to acquire things, from the major end item, weapons system major-milestone process that we use.

I mean, the cute little example I use is it takes us, on average, 81 months to field an IT system and Apple fielded the iPhone in 24 months. Well, it takes me 24 months to get a budget approved for a system. So it's not really fair that Steve Jobs gets an iPhone and I get a budget. (Laughter.) It's not the same.

And then there are broader – we have some broader efforts to see if we can, just, fundamentally attack the paradigm for manufacturing technology and change, by an order of magnitude, the time. Now, that's a long-running project and I'm not sure we're going to see immediate results from that.

But with all that said – acknowledging the challenges of that – those challenges have existed for decades and we still have the best military in the world. So as much as they exist for us, in general, they're worse for other people. So in that sense, it's a relative game that you're playing here, and we need to make sure that we're able to at least stay ahead, I think, is a goal. But the longer-run goal is to fundamentally improve the system. Let me go all the way in the back. Behind you, I'm sorry.

Q: Hi, Robert Schroeder of International Investor, representing a little bit more the business and financial interest in communities, especially – I'm glad you brought up cyber war

because we have been hearing some anecdotal evidence that some of the attacks that have been launched against the business communities have been reciprocal in nature.

From their understanding, at least in some of these investigations, the countries that have launched these attacks are claiming that they, themselves, have been the victims of attacks launched by our government. Can you tell us, has the Defense Department been probing or launching any cyber attacks on other nations just to see how weak or strong their defenses are?

MR. LYNN: As I indicated, the U.S. is more dependent on information technology, for both its security and its economy. As a consequence, the focus of our efforts is on defending our networks. I think we've done a reasonable job, in the last couple years, in terms of increasing the strength of our military networks.

We're working with homeland security on a plan that will extend protection to our government networks. And we're at the first stage of working with homeland security in looking at what kinds of protections that we can offer critical infrastructure, as well. And by that, I mean transportation, power grid and so on. At the end of the day, the U.S. is the most dependent on IT and we need to act that way. Let me – I'm going to go over here.

Q: Hi, Alex Baca (sp) from Northrop Grumman. My question is, based on the last question that was asked, it sort of tells you that your notion pushes you, on the one hand, to very responsive acquisition systems, very quickly procured – things like IED, where you field them very quickly and they become obsolete very quickly as the threat evolves and you have to go off and get new things.

But the other sort of interpretation of the sort of future you laid out is that you're looking for programs like the next B-52 – something that is infinitely configurable, very adaptable to very different kinds of missions and stays in the inventory for, sort of, you know, 50 or 60 years. And as you start to think about how you want to, you know, reconfigure the DOD and re-equip the DOD, are you thinking more in terms of solutions that are like the B-52, where you can apply them to everything, or are you thinking in terms of more, like, lots of very quickly procured point solutions that are responsive to the threats as they evolve and they happen?

MR. LYNN: I don't see how you could choose between those two. I think you're going to have to do both, and how much of each you do is going to depend on your assessment of the threat and the trends that I laid out. I think in some cases with – you know, certainly with bombers, we kept them far longer than we expected to but we have modernized them several times over. With aircraft carriers, sort of a similar story.

With other things, as you said, whether it's communications gear, cyber equipment, some counter-IED technology, you have to have a much faster replacement rate. And I just think the challenge is to define which things fit in which category, but I don't think you can go to a one-size-fits-all approach. Let me go to this side, here. This is just to make the people with the microphones run. (Laughter.)

Q: My name is Nathan Tabes (ph) from the Center for Justice and Peacebuilding. And you've talked about the weakness of not being able to predict where conflicts and where we're going to be fighting in the future. But all the solutions that are being talked about here are how we can continue to fight and be on the defensive or the offensive – however it may be – and thus, continuing to keep making the same mistake of not being able to predict where those are.

So why aren't we putting more energy into trying to figure out where those conflicts might be instead of more technology into continuing to protect ourselves from the same mistakes that we might make? Am I being clear?

MR. LYNN: Well, yeah, although I think I'd answer a little bit along a different line. We are investing – we have very large investments in the intelligence arena, both open source and less open approaches, and we do try and do the best we can, and hopefully, we'll get better. I think, to pivot off your question a little bit, I think the stronger approach, though, than to try and predict them, which, as I suggested, I think it's going to be very difficult to get much more successful than we've been.

I do think we might have more success in preventing conflicts, and that means more front-end investment that's more heavily State Department-focused, or is a partnership between State and Defense on things like security assistance, economic development, improvements in governance. And the hope would be that you would head off crises before they reach the stage where the U.S. was needing to deploy military forces – that you've addressed the problems in advance.

That's a little bit different than predicting them. It's more looking across the scope of the challenges you face, identifying the ones that might become cauldrons of conflict – and not necessarily trying to identify which is going to be the conflict – but try and address the panoply of them and bring them all back down from a boil so that we won't have to, as I say, deploy military forces.

I think I should add, though, I think that is going to be a particular challenge in the fiscal environment that we face because, as I indicated, defense is clearly going to be part of an overall reduction in government spending but there's generally strong constituencies for defense spending. For the kinds of security assistance, economic development spending that I think is critical to that prophylactic impact that I was talking about, I think the constituencies are much weaker and they may suffer in a fiscal tightening that we're in. Let me go back.

Q: Arnaud de Borchgrave, Mr. Secretary, CSIS. Adding to your dramatic examples of what happened in the last century, from the time the Germans were dropping bombs by hand from biplanes in World War I until we dropped the big one on Hiroshima was only 28 years. So my question is, how long do you think it will be before we move into something that could be called robotic warfare?

MR. LYNN: I mean, it's hard to say. I mean, I tried to suggest in there things have moved – as you just suggested, things have moved faster than people generally project at the time. And so I think with robotics; I think with cyber; I think possibly with, you know, things

like composite materials; with fuel cells – all of those are potentially revolutionary technologies. I think at least some of them, maybe not all of them, will move faster than we anticipate.

And so I think our planning needs to try and take account of that and we should try and be at the outer edge of this development, rather than waiting and seeing. So I can't give you a timeline but I think we need to plan with the anticipation that we don't know what the timeline is, but whatever it is, it's likely to be faster than anything we have projected. I want to go to the corner – yeah, to my right.

Q: Thank you. My name is Maggie Chin (sp) with the Voice of America, Chinese service. Thank you so much. My question is regarding U.S. arms sales to Taiwan. It's one of the most sticky points between the relations of the United States and China, but however, the administration has faced a huge pressure from the Congress to push toward such sales and to abide by the Taiwan Relations Act. So I would like to get your take on the upgrade of F-16A/B and the sale of F-16 fighters. And if I could get a timeline of that, that would be great. Thank you.

MR. LYNN: Well, I think where you're going is the underlying relationship between the United States and China, and we just recently had a visit. Admiral Mullen hosted his counterpart from China and Admiral Mullen is hosting to reciprocate that visit to China, and we think that, that will help build up the relationship between the two militaries, as we've built up the economic and diplomatic interaction between the two nations.

As you indicated, there are always going to be issues between the two great nations where there are disagreements. I think the challenge is going to be to maintain a positive relationship going forward despite those agreements. And I think that the kinds of steps that have been taken most recently suggest that we are at least taking some small steps down that path. Right where you are, on the aisle.

Q: Mike Wheeler, Institute for Defense Analyses. Thank you, Mr. Secretary, for your very cogent comments. My question is triggered by what Admiral Denny Blair testified on two weeks ago – his first appearance since he left the office of DNI – and he was advocating creation of Title 60 to reflect the reality that the clandestine service, cover operations and the military department Special Operations are increasingly integrated as an arm of warfare.

My question isn't so much Title 60 but it's where this all is going. Do you see this as another strategic trend which is going to affect how the United States conducts warfare and, perhaps, has warfare conducted against it, not only at the low end of the spectrum but potentially at the high end of the spectrum, as well?

MR. LYNN: I guess I wouldn't put it, no – I mean, I think the split between Title 10 and Title 50 is – I don't think I would put it in a strategic trend. That's a U.S. construct. That's, you know, the split that we have between our intelligence functions and our military functions. You're always going to have seams and you're always going to find situations when you have a legitimate choice to choose either and you have to set up a construct for how you're going to make the choice between using intelligence and using military assets.

I agree with Admiral Blair that I think we could improve that construct, particularly as we get into newer forms of warfare, but I think it's probably too far to think that we – as with anything, that you're going to eliminate the seam. You can move it. You can make the criteria by which you choose clearer. But at the end of the day, you will not be able to eliminate the seam. You won't be able to eliminate the necessity, at the end of the day, for the president or others to make those choices.

Q: Thank you for the opportunity. My name is Suraya Sadeed. I'm the executive director of Help the Afghan Children. I just want to know if, given the fact that there's a ghost war going on in Afghanistan and the conventional wars are obsolete, what will be the next step that the United States will take in Afghanistan? Thank you.

MR. LYNN: Well, I mean, I think we're in the midst of the beginning of the next step. General Petraeus will make recommendations in the very near future about how to implement the phased drawdown that the president announced almost 18 months ago. I think it will be, as the secretary and the president have talked about, it will be conditions-based.

It will depend on judgments about the strength of the Taliban, about the progress, in terms of the capabilities of the Afghan National Security Forces and the ability of the Afghan government to take an increasingly larger role in the security function. So I think that shift will start very soon and will progress over the next couple of years to that full transition that's projected for 2014.

Q: Good morning, Mr. Secretary. Paul Sullivan, USEC. You discussed in your talk the need to balance agility and flexibility for future wars that you just don't know how they're going to start, and then you have to balance that against the long-term, 10-year, 12-year wars. Those are conflicting force structures and organizational challenges. Do you foresee any changes in any of the military departments or in the DOD organization to facilitate rapid or flexible balancing of those two conflicting concepts?

MR. LYNN: I guess in the thrust of my comments was that it's – I think you're right that the high-end, near-peer-type preparation is quite different than the lower-end counterinsurgency. There's some overlaps in terms of lift and intelligence/surveillance/reconnaissance assets, but a lot of it is different.

I guess what I was trying to do with the thrust of my comments was I think you can decide which of those two you want to emphasize. I don't think you can eliminate either. I don't think you can go to the extreme, as I think some have suggested, that we should just abandon one or the other. I don't think that's possible. I think it's going to be less satisfying than that. I think it's going to be a matter of emphasis rather than choice.

Q: Gene Procknell (sp) at Deloitte. You suggested areas we're going to have to add funds, invest in, in terms of asymmetric warfare, cyber – places where we're going to spend more money over longer durations. How about the flipside? How can we afford that? What

things can we end? What missions can we end? How are we going to get the cost savings to fund those kinds of needed investments?

MR. LYNN: That's one of those questions that makes it to the deputy. (Laughter.) It only goes to the deputy and doesn't get either – either side of me doesn't answer that. I mean, we've laid out a process that, we're trying to do exactly that. I mean, obviously, the first choice of everyone is to try and gain further efficiencies. The effort Secretary Gates led over the last year yielded $178 billion, largely in reductions in overhead, headquarters systems at the lower end of need.

I think we can find more in that. The president has laid out a goal of $400 billion. To be frank with you, I don't think we're going to find $400 billion of pure efficiencies – and by pure efficiencies, I mean things where you're able to do the same thing or the same mission, just for less – for less resources, fewer people and so on. I think there's some of that out there.

I think, you know, for example, cloud computing offers some potential in that regard. You can get the same or greater capability with less equipment, with fewer support. But that's going to be limited so we're going to have to – I think we're going to have to do things like make the choices that we were talking about with the prior gentleman – you know, which end of the spectrum do you want to emphasize? Not to exclusion of the other, but which end are we going to emphasize? I think there's some important judgments there.

I think, as in all of the government departments, we're going to get into some very politically contentious things – things that we would say are not justified on the merits but seem to have strong constituencies or the justification on merit doesn't rise to the level that we'd fund them. And I think a little bit the debate on the alternate engine presages that.

I mean, it's the department's judgment that it is not worth the $2.9 billion investment up front in this fiscal environment for a very, very uncertain benefit over, frankly, decades. But there's a constituency for that, and so we're – it's a very difficult challenge. I think we're going to see many more of those and we're going to have to make those hard choices if we're going to reduce defense spending.

Q: Thank you, Mr. Secretary. (Inaudible, off mic.) In the future, do you see privatization of contractor capabilities in the military, both – (inaudible, off mic)?

MR. LYNN: I mean, I think in the '90s, for a variety of reasons, we over-steered on privatization. We thought it applied to everything. And so we – in a relatively-across-the-board way, we pushed all sorts of functions out, I think, without appropriate consideration for whether those functions should be retained in the government or whether they should be privatized.

I think over the past couple of years, we've tried to rebalance and to make those judgments and to pull things into the government, such as acquisition oversight, where we think that there really is a government function or where you need a certain critical mass of expertise in the government just to be a smart buyer – just to be able to bring value to the government.

So I think we need to make those judgments going forward, so it's going to have to be more nuanced. I don't think you're going to see a big shift to privatize that you saw in the '90s. I think that, you know, there was – at the beginning, a couple of years ago, there was more of a pull to bring things in. I think this has rebalanced a little bit.

We're, I think, targeting things that we want to bring in but we're trying, again, not to do it in a – trying to do it based on the analysis of the merits of the individual function, rather than doing it across the board when, either, you're bringing things in or pushing things out.

Q: Thank you, Mr. Secretary. My name is Tiffany Chow and I'm with Secure World Foundation. Many of the evolving threats you mentioned here, especially in the space and cyber environments, defy classic deterrence theory and strategies. What is the Defense Department doing to develop and define its so-called red lines in the information age, and how can we make these clear to our adversaries?

MR. LYNN: I mean, it's an interesting question as to how deterrence theory applies in these areas, such as cyber. I mean, in cyber, attribution is enormously difficult. I wrote in an article earlier that in the missile age, you know, missiles come with return addresses so you pretty much know who launched it. Cyber attacks – it's not nearly as clear.

And then, as I suggested in the remarks, you may be facing terrorist or criminal groups who have no assets to deter. So you know, the classic deterrence theory, which was represented by, you know, mutually assured destruction, doesn't work very well if you don't have attribution and the other side doesn't have assets.

There is a different, though, theory of deterrence that can apply here, which is denial of benefit. If you're able to strengthen your defenses in a way, in cyber and other areas, such that it is either – you've so raised the costs of an attack that it makes it less interesting and the adversary goes on to other areas. I think that, that is indeed the path that we're going to have to proceed down, is we're going to have to be able to deny benefits to attackers in cyber.

MR. : Last question.

MR. LYNN: Okay, let's see. The winner is – I skipped over you, so let me – I think they thought –

Q: Thank you, sir. Akira Chiba, Japanese Embassy. On the budgetary aspect of warfare, I was told the other day that if you don't have enough money to spend yourself, let your adversaries spend and go into shopping sprees so that it will lead them into bankruptcy, and it's called the cost-imposing strategy. And I think that Star Wars resembles that. Now, if you look at the huge deficit that your government is suffering today and if you look at who is buying all these Treasury bonds, do you see any conspiracy somewhere in there? (Laughter.)

MR. LYNN: Yeah, by most of the people in this room. (Laughter.) I mean, the theory is – I mean, as it went in the '80s and '90s – that theory was called competitive strategy. It was the idea of imposing costs on your adversary. So you know, Star Wars is one; air defenses is

another. I think you certainly have to, you know, look at what the relative costs are but at the end of the day, the primary judgment is what is needed for U.S. national security and how do we afford that.

And we have to balance the fiscal needs that I started the talk with. But I don't think we cannot buy things because we don't think the relative cost versus the adversary is in the right balance. I think we're going to have to try and meet the national security needs within the fiscal constraints we have, and that's the core set of judgments, rather than trying to play a game with comparative costs.

MR. HAMRE: If you'll indulge me, one last question.

MR. LYNN: Sure.

MR. HAMRE: They're paying for the ballroom, so I'm going to let them do it.

MR. LYNN: I see. (Laughter.)

Q: (Inaudible, off mic.) Brian Barwich (sp), Finnmeccanica, U.K. Mr. Secretary, in addressing the threats that emanate from the trends in warfare that you've outlined, what are your assumptions and what are your expectations of allies and international partners?

MR. LYNN: I mean, that's a great question. I mean, we obviously have enormous fiscal challenges and we're in the midst of trying to wrestle with them. I would say Europe is probably a little bit ahead of us in that regard and has already started to make hard decisions.

I think our expectation and hope is that, as our allies and international partners wrestle with their equally tough fiscal challenges, that they will, you know, keep in mind the importance of the security dimension and ensure that the core functions and missions that the NATO alliance and the other partnerships that we have are protected, even as they do so with devoting fewer resources.

MR. HAMRE: Let's thank Secretary Lynn for a very, very interesting conversation. (Applause.) We're going to take about a 15-minute break. We now break into three parallel sessions. This session is going to be the energy discussion. On the same level is going to be the simulation. And then upstairs is going to be the cyber discussion. Thank you.

(END)