

**CENTER FOR  
STRATEGIC AND INTERNATIONAL STUDIES  
(CSIS)**

**PROTECTING THE DOMAIN:  
CYBERSECURITY AS A DEFENSE PRIORITY**

**WELCOME:**  
JOHN HAMRE,  
PRESIDENT AND CEO,  
CSIS

**MODERATOR:**  
JAMES LEWIS,  
DIRECTOR,  
CSIS TECHNOLOGY PROGRAM

**SPEAKER:**  
WILLIAM J. LYNN, III  
DEPUTY SECRETARY,  
U.S. DEPARTMENT OF DEFENSE

**MONDAY, JUNE 15, 2009**

*Transcript by  
Federal News Service  
Washington, D.C.*

JOHN HAMRE: Good morning, everybody. Glad to have you here. This is – it gives you a sense of the importance of this topic that so many people want to be here. I will say, Melissa, there are more people here than there were for you on Friday, but that was Friday afternoon, and that's – we understand. And you did a fabulous job. Thank you for laying out the framework, you know, that the administration's identifying. It was a terrific presentation.

We're going to hear today from Bill Lynn. I will tell you I have – well, I can't tell you how far back our histories go, because they are entwined back to many, many years when we worked together up on the Hill. I had the privilege of working with Bill when we were in the government – when I was in the government the last time, and at that time he was initially the head of PA&E and just did a terrific job, and then became the comptroller, and was absolutely the logical person to become the deputy secretary. I'm so glad that that's worked out.

I know how broad his portfolio is. And so I'm delighted that he is personally giving time to dig into a topic this important. I think it's emblematic of how seriously the administration is now taking the question of cybersecurity that the deputy secretary is going to be making it a focus.

And so, Bill, we're delighted you're here. This is – I will tell you this is a dangerous audience, so be careful. No, I'm teasing. This is going to be – it's a fabulous audience. I'm glad you're here.

Ladies and gentlemen, the deputy secretary of Defense, William J. Lynn.

(Applause.)

WILLIAM J. LYNN: Thanks very much, John.

As John said, our history goes way back. In fact, it goes back to the time I was actually here at CSIS, fresh out of graduate school, working on a Goldwater-Nichols study. And one of the senior members of the study was Alice Rivlin, and she brought along her best young defense analyst at the time; wouldn't go to any meetings without him. That was John Hamre.

And since then I've been following John. John went to the Senate, the Senate Armed Services Committee. So I couldn't get on the full committee, but I got on Senator Kennedy's staff working on the committee. And then John went to the Pentagon and became comptroller. As John said, I went to the Pentagon as PA&E, but when John moved to deputy secretary, I moved up to be comptroller following John. And then in this most recent job, I am again following John as deputy secretary of Defense.

So I'm looking forward to getting inducted into the South Dakota Hall of Fame – (laughter) – because that seems to be the only thing John's done that I haven't followed him on. And so I'd appreciate your letter in that regard, John.

John, but still, at every step you've set the standard for public service. And those of us at the department continue to rely on John, as he chairs the Policy Board. And I want to thank

you, John, for your friendship, but more importantly, for your leadership, more than 30 years of leadership in public service.

And the rest of you at CSIS, thank you, as well, for your leadership. You really set the standard in bipartisan policy advice and policy direction.

I come to you today on behalf of an administration that's seeking that same bipartisan problem-solving spirit. We have a president who, in one of his first acts in national security, reached across the aisle and chose the secretary of defense from his previous – from the previous administration, a secretary from another party. In Secretary Gates, we have a secretary who, in his long career here in Washington, has worked for eight presidents of both parties.

This bipartisan approach, I believe, is the reason we've been able to use these first few months not merely to tread water, which is the usual criticism of a new administration's early budgets and policy decisions, but really to make some of the hard decisions in the defense budget and try and start pursuing a new direction in defense.

To keep our armed forces the best-trained, the best-equipped, the best-led military in the world, we're increasing the defense budget between fiscal '9 and fiscal '10. To ensure our forces can meet today's missions, especially in Iraq and Afghanistan, we've halted any personnel reductions in the Navy and the Air Force, and we've achieved increases in the Army and the Marine Corps, and we've done that two years ahead of schedule.

To give our warfighters the tools and the technologies they need when they need them, we're making major reforms. We've cancelled unproven weapon systems, we're investing in weapon systems we know that work, and we've launched a series of initiatives to finally bring us true acquisition reform.

And to better prepare our forces for the range of challenges they'll face, the conventional and the unconventional and the hybrid warfare that combines them both, we're making irregular warfare a regular part of America's military planning.

As the president said at the Naval Academy, quote, "We must overcome the full spectrum of threats. This includes the nation-state and the terrorist network, the spread of deadly technologies and the spread of hateful ideologies, 18th century piracy and 21st century cyberthreats."

It's that last challenge that brings me here today, although standing in front of this crowd I'm reminded of the old story of an individual who passed and went up to heaven, and he had been – had a – the defining experience in his life had been surviving a flood. Whenever he was asked to speak, that's what he spoke about.

So when he gets to heaven, Saint Peter says, well, looking good for your admission, but you're going to have to make a speech to the rest of the team up here. He says, no problem, I'll

talk about my experience in the flood. Saint Peter said, well, that's fine, but recognize Noah will be in the audience. (Laughter.)

I noticed all the arks parked out in front, and I know I've got a lot of Noahs, when it comes to cybersecurity, in this audience. Many of you have been dealing with this issue for years – in government, in industry, in academia – so I won't presume to educate this audience.

But I do believe today's an opportunity to deepen our understanding of this issue, because in recent months we've taken new steps to meet the challenge. Starting with Jim Lewis – and the CSIS Commission on Cybersecurity issued its report last December. I think that's become the touchstone document as people have looked this year at the new challenges of cybersecurity. I want to commend Jim, you and your team, for that terrific effort.

In April, a panel of the National Academy of Sciences issued a draft report on cyberthreats and how we might respond. More recently, the president just completed his 60-day review, coming into office, of the cybersecurity arena. And I want to recognize Melissa Hathaway for leading us through that difficult interagency thicket and bringing out a really solid report that's, I think, going to set the agenda for President Obama's term, on terms of how he deals with cybersecurity and securing America's digital infrastructure.

Each of these efforts offered a broad range of recommendations. But there was one recommendation that they all shared: The need for greater public awareness of the cyberthreat to our country and how we can protect ourselves.

So today I want to speak about what this challenge means for the Department of Defense. And I want to be very clear about this. Even though it risks stating the obvious, I'm the deputy secretary of Defense; I'm here to focus on how the Department of Defense protects and defends the Defense and military computer networks: what we're facing, what we've done so far, what we're doing today, and what we need to think about going forward.

Just like our national dependence, there is simply no exaggerating our military dependence on our information networks. The command and control of our forces, the intelligence and logistics upon which they depend, the weapons technologies we develop and field, they all depend on our computer systems and networks. Indeed, our 21st-century military simply cannot function without them.

Not surprisingly, our networks, some 15,000 of them – including some 7 million computers, IT devices, laptops, servers – all make for a tempting target. But this is not an emerging threat. This is not some future threat. This cyberthreat is here today. It is here now. In fact, the cyberthreat to the Department of Defense represents an unprecedented challenge to our national security by virtue of its source, its speed and its scope.

There's the source. The power to disrupt and destroy, once the sole province of nations, now also rests with small groups and individuals, from terrorist groups to organized crime, from hacker activists to teenage hackers, from industrial spies to foreign intelligence services.

We know that foreign governments are developing offensive cybercapabilities and that more than 100 foreign intelligence organizations are trying to hack into U.S. networks.

We know, as Director of National Intelligence Dennis Blair has stated, that both Russia and China have the capability to disrupt elements of other nations' information infrastructure. We know that organized criminal groups and individuals hackers are building global networks of compromised computers, botnets and zombies, and then selling or renting them to the highest bidder, in essence becoming 21st-century cybermercenaries.

We know that terrorist groups are active on thousands of Web sites and that al-Qaida and other terrorist groups have expressed their desire to unleash coordinated cyberattacks on the United States.

Next, there's the speed of the threat. As I believe John Hamre noted when he was deputy secretary, in the 18th and 19th century we faced a threat where ships crossed the ocean in days. In World War II, aircraft could cross the ocean in hours. In the Cold War, missiles could do it in minutes. And now today, cyberattacks can strike in milliseconds.

Such speed has profound implications for how we protect the department's networks. If attacked in milliseconds, we can't take days to organize and coordinate our defenses. If our networks to be – were to be disrupted or damaged, we'd need to respond rapidly, at network speed, before the networks could become compromised and ongoing operations or the lives of our military are threatened. In short, we have to be just as fast or faster than those who would do us harm.

Finally, there's the scope of the threat. Instead of simply keeping adversaries out of our homeland, we have to prevent large-scale cyberattacks inside the homeland, inside the networks. Consider the main targets, which loosely mirror the three domains dot-mil, dot-gov and dot-com.

First, dot-mil. We face attacks, as I've said, on military and defense networks, perhaps with the intent to disrupt military operations. As Secretary Gates has said publicly, our defense networks are constantly under attack. They are probed thousands of times a day. They are scanned millions of times a day. And the frequency and sophistication of attacks are increasing exponentially.

As the president acknowledged last month, we experienced one of the most significant attacks on our military networks last year. Several thousand computers were infected by malicious software, forcing our troops and defense personnel to give up their external memory devices and thumb drives, changing the way they use computers every day.

Fortunately, cyberattacks on our military networks have not cost any lives – not yet. But they are costing an increasing amount of money. In a recent six-month period alone last year, the Defense Department spent more than a hundred million dollars defending its networks. Guided by last year's comprehensive national cybersecurity initiative, the

department is spending billions annually in a proactive effort to protect and defend our networks.

Second, dot-gov. Here we face attacks on civilian government networks, perhaps to slow our response in a crisis. We see the risk every day, with federal networks being breached thousands of times. We have seen the networks of foreign governments, such as Estonia and Kyrgyzstan, crippled by denial-of-service attacks. And during last year's Russian invasion of Georgia, we saw cyberattacks shut down Georgia's government and commercial Web sites. A military attack on – alongside cyberattack is the very definition of hybrid warfare.

Third, and most broadly, dot-com. These include attacks on our privately owned critical infrastructure, transportation, telecommunications, power and financial grids on which our national security and the economy depend. Already, cyberattacks have taken down power grids in other country (sic), knocking the lights out in multiple cities.

Likewise, attacks are on the rise against our defense contractors, who face cyberespionage from foreign governments, competitors and criminals. Indeed, major aerospace weapons platforms have experienced intrusions that have compromised unclassified but sensitive technical information.

For all these reasons, the president last month called the cyberthreat, quote, “one of the most serious and – one of the most serious economic and national-security challenges we face as a nation.”

So what are we doing, to confront this challenge, at the Department of Defense? The American people and our men in uniform should know – men and women in uniform should know this.

Starting in large part with John Hamre's efforts, in the late 1990s, the department has built strong, layered and robust cyberdefenses. The 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 need to protect.

Just as we need freedom of navigation of the seas, we need freedom of movement online. Just as we protect the front gate at military bases, we must protect the back doors, the systems and networks that our adversaries seek to exploit.

This is not some expansion or extension of our mission at the Department of Defense. On the contrary, it is keeping with our defined and historic mission, to protect and defend our national security and to protect the lives of our men and women in uniform.

So the Department of Defense will defend its computer networks. We will protect this domain. Just as the president has called protecting the nation's networks a national security priority, protecting our defense networks is a defense priority.

To this end, the Office of the Secretary of Defense, our undersecretaries of Policy, Intelligence and the chief information officer provide the civilian oversight of our cybersecurity policy.

The national military strategy for cyberspace operation, developed by the chairman of the Joint Chiefs of Staff, lays out our strategy or ensuring our cybersecurity. And the military services, each have organized themselves accordingly.

The Army has created the Network Enterprise Technology Command in Arizona. The Navy has created the Naval Network Warfare Command in Norfolk. And soon the 24th Air Force, based most likely at Lackland Air Force Base in Texas, is being stood up.

And day-to-day responsibility for operating and defending our defense networks rests with the U.S. Strategic Command, STRATCOM. In this mission, STRATCOM receives critical support from the National Security Agency and from the Defense Information Systems Agency, two organizations that have long been responsible for building, operating and protecting the department's information systems.

And to insure the sensitive defense information, on the unclassified networks of our industry partners, we're proceeding with our Defense Industrial Base initiative, the DIB. We're working more closely than ever before with our defense contractors, sharing critical information on the latest cyberthreats and vulnerabilities, reporting incidents quicker and moving faster to respond and recover from attacks, as we did with the recent Conficker worm.

Together these efforts are why the CSIS report found that along with the intelligence community, the Defense Department is the best-prepared agency, when it comes to cyberdefenses. That said, we need to do better. In his remarks last month, the president warned that as a government and as a country, we are not as prepared as we should be.

The same is true of the Department of Defense. That is why cybersecurity is a central focus of the ongoing Quadrennial Defense Review. And that is why we need a doctrine to govern how we protect cyberspace, as a domain, how our forces are designed and trained to protect our networks.

The QDR will assess our current capabilities against this requirement and make recommendations for the future. But before even completing the QDR, we're pursuing a number of initiatives. These fall into three areas: culture, capabilities and command.

First, building a culture that makes cybersecurity a priority. We need a cadre of cyberexperts, who are trained and equipped with the latest technologies, to protect and defend our systems.

Yet today, our military schools only graduate about 80 of these experts per year. So our budget for fiscal year 2010 includes funding to more than triple the number of experts we graduate, to 250 per year.

More broadly, in the department there are an estimated 90,000 personnel engaged in administering, monitoring and defending our 15,000 networks, but most are not formally certified in information assurance and cybersecurity. So we're proceeding with a training and certification program to build a truly world-class cyberforce.

And across the entire department, we're improving cybersecurity training, awareness and accountability for the more than 3 million military and civilian personnel who log onto military networks every day because, as General Kevin Chilton of STRATCOM has said, every network computer is on the front line, everyone who logs on is a cyberdefender first.

Second, we're improving our capabilities. Before we ever deploy our weapons systems into the field, we have subjected them to extensive tests and evaluations. Before we ever send our troops into battle, we test their skills and tactics on training ranges. Yet, we have no such equivalent in cybersecurity. So DARPA, which helped invent the Internet decades ago, is leading our effort to build a national cyber range – in effect, a model of the Internet. This will allow us to engage in real-world simulations and develop tests and field new leap-ahead capabilities for cybersecurity.

As we build these capabilities, I would suggest that we must resist the temptation and the false comfort of trying to retreat behind a fortress of firewalls. Today's cyberthreats are organic and are constantly evolving. Our cyberdefenses must do the same. We can't afford a digital version of the Maginot Line, that static French defense of World War II that the French assumed would work – excuse me, static French defense of World War I that the French assumed would work in World War II. Instead, we need to remember the lessons of maneuver warfare, from the Second World War to Operation Iraqi Freedom, where new tactics and technologies allowed nimble and agile forces to out-manuever their adversary.

The third area in which we're taking action is command. Despite our progress at the department, we need to even better – we need to be even better at detecting and defending against cyberattacks. We need to do it faster, at network speed. We need more people assigned and trained for this mission, and we need to end the jousting and jockeying within the department for personnel, for resources, for authority, that has often prevented a more coordinated and effective response to the cyberthreat.

As you have no doubt heard, we are considering the creation of a new command, a subordinate unified command under STRATCOM to lead, integrate and better coordinate the day-to-day defense and protection of our defense networks. As of today, Secretary Gates has not made the final decision on this command, but what I can tell you is this. Such a command would not represent the militarization of cyberspace. It would in no way be about the Defense Department trying to take over the government's cybersecurity efforts. On the contrary, such a command would not be responsible for the security of civilian computer networks outside the Defense Department.

Its mission would be to protect and defend our defense and military networks: "dot.mil." Responsibility for protecting federal civilian networks would remain with the

Department of Homeland Security. Likewise, responsibility for protecting private-sector networks would remain with the private sector.

Like other commands, a new command would be responsive to congressional oversight, would operate within all applicable laws, executive orders and regulations. What the president said last month of cybersecurity efforts across the government applies equally to our efforts at the Department of Defense. We can and we will protect our national security and uphold our civil liberties.

At the same time, we're mindful of the challenges ahead. We've marked the hundredth anniversary of military aviation but, by comparison, this year marks only the 20th anniversary of the World Wide Web. And as I've described, in many ways, as a country, as a government, we're still in the early stages of getting organized. Indeed, how we ensure our cybersecurity in the decades ahead will depend on how we answer key questions.

For example, within the Department of Defense, what are the rules of the road? As the CSIS report noted, there are a whole host of questions that we face. How can we deter and prevent attacks? Deterrence is predicated on the assumption that you know the identity of your adversary, but that is rarely the case in cyberspace where it is so easy for an attacker to hide their identity.

Beyond the military, how do we organize government as a whole? The president will name a cybersecurity coordinator at the White House to coordinate efforts across the government. And as I've said, the Department of Homeland Security will remain the lead for protecting federal civilian networks. And yet, given the imperative of defending government networks, it would be inefficient – indeed, irresponsible – to not somehow leverage the unrivaled technical expertise and talent that resides at the National Security Agency, which has so much experience protecting our national security systems. What we must do, of course, is to apply that expertise in a way that upholds and respects our civil liberties.

Beyond our own government, how do we cooperate internationally? Many of the cyberattacks on U.S. networks originate overseas. Botnet attacks involve computers all over the world. How we protect and defend ourselves in the global – in this global environment raises complex questions of national sovereignty and international law, and no single government would be able to confront these complexities alone.

Finally, beyond government, how do we partner with industry? Neither government nor the private sector can solve our cybersecurity challenges alone. Government needs industry, which owns and operates most of the nation's information infrastructure. The private sector needs government – the government to establish coherent, effective and transparent laws and regulations. Yet, the difficulties of forging genuine public-private partnerships in this area are well known. Fundamentally, it comes down to trust: industry needs to trust government to protect its proprietary information; government needs to trust industry to protect its classified information on threats and vulnerabilities. Meanwhile, more adversaries are targeting our systems, more networks are being breached and more information is being compromised.

The Defense Industrial Base Initiative I mentioned is one model of a new approach where government and industry come together to share information and strengthen our cyberdefenses. There are other models. And I would say to all of you here today – from industry, from academia – we need you to help us find the right model so that we can forge real partnerships of trust and cooperation that protect our security and our prosperity, because that in the end will be the only way that we’ll meet the challenge, with partnerships of trust; the best minds in government and industry and academia here in the U.S. and around the world, working together.

That, as General Keith Alexander of the NSA has noted, was how the Allies broke Germans’ Enigma encryption during World War II. That, as John Hamre knows from personal experience, was how we avoided the potential catastrophe posed by Y2K. And that is the spirit that we’re committed to at the Department of Defense.

Working together, we can bring real cybersecurity to cyberspace. We can and we will protect our national security and our civil liberties, without compromising either.

Thank you very much for your attention.

(Applause.)

JAMES LEWIS: Okay, great. Well, we have time for a few questions.

Let me thank the deputy secretary first of all for really an excellent speech – really an excellent speech. And I know some of us in the room – we were talking about people who – I don’t know if I want to be Noah, but the line about maneuver warfare versus the Maginot Line I think was exactly right. And thinking what that means in cyberspace is crucial, but also difficult.

But with that, let’s see if we have some questions. We have a few minutes. Go ahead, with the green shirt, please.

Q: Yeah, please –

MR. LEWIS: And could you identify yourself?

Q: Dave Fulghum, with Aviation Week. Working from the premise that a good defense is a good offense, do we have a functional system now to get approval for electronic tag? Does that process change in wartime or military emergency? And how are you going to come up with a tactical decision system that’s going to be fast enough to get inside the bad guys’ OODA loop?

MR. LYNN: Well, one of the reasons we’re looking at a Cyber Command, as a sub-unified command of the Strategic Command, is to unify all aspects of cyberdefense; so that you don’t separate out offense, defense intelligence; so that all of the – all various aspects work together.

And the kinds of questions that you're asking are exactly the ones that this sub-unified command would address, assuming that it's set up in the near future.

Q: Is the answer then, we can't do it yet.

MR. LYNN: The answer is what I said.

(Laughter.)

MR. LEWIS: Next question. We have one in the back.

Q: Tony Capaccio with Bloomberg News.

What initiatives are you taking to force better reporting, by defense companies that have been intruded on with sensitive but unclassified information? Is there any proposed DFARS regulation to stiffen compliance and potential penalties, if they don't report in a timely manner?

MR. LYNN: As I said, I think that the best way forward here is a partnership between industry, the defense industry, and the department, where we're mutually sharing information, and that gives the kind of information that you just talked about, and where we give information about the threats as we see them.

I'm not aware of any regulations to put that into effect. As I said, we've set up this Defense – the DIB. There are some other industry groups. I think cooperation and collaboration is increasing.

And we're hoping that we can build on that foundation, to have a full and frank exchange, and that people will feel confident that their proprietary information won't be compromised, and that the government can feel confident that classified information won't be disseminated, outside of classified channels.

Q: (Off mike.)

Have you noticed that there's been a problem though, with underreported incidents that you learn about belatedly?

MR. LYNN: I can't think. It's possible, but I can't think of – certainly not in the last few months can I think of any examples. Whether it happened before, I don't know.

I think this is an evolving area. It's possible it's happened before. I think people have to step into this collaboration. But I think it's going quite well right now.

MR. LEWIS: Two up in the front here.

Q: Eric McVadon, The Institute for Foreign Policy Analysis.

Mr. Secretary, I wonder if you'd elaborate on the international aspects of this. Are we maybe using alliance, like NATO and the U.S.-ROK and U.S.-Japan alliances, as a vehicle? Or is there a need, because all of us are facing this problem, to look at it in a bigger way and see if we can bring some sort of structure together, for cybersecurity, maybe even including a country like China?

MR. LYNN: You're absolutely right.

The international component, as I probably alluded to too briefly in the prepared remarks, is a critical element of this. There are, I think, some nascent international organizations. There's a cybercrime focus in Europe that's made progress.

There are – some progress is being made on some standards. But I think it's still episodic. And there needs to be, I think, a more coherent and structured effort. And that's one of the things. Pursuit of the recommendations out of the president's 60-day review, I'm sure, will be one of the major thrusts.

MR. LEWIS: Okay. How about over there, please.

Q: (Off mike.)

Mr. Secretary, in terms of China, there's been a lot of news of attacks from there. Is it mostly coming from the government and military? Or is it from independent hackers?

MR. LYNN: Well, as I indicated, one of the new things, about this world, is the difficulty of attribution, so that you can trace it back, to places in China, but it is difficult to attribute the who and who is behind it. And I think that's where we are, with those kinds of attacks.

We've traced it back. Some of the attacks we've traced back to China. But we are not at this point able to attribute whether it's a private, public, whether it's military, intelligence, industry or criminal.

MR. LEWIS: Maybe one in the front.

Q: Hi, Mr. Secretary. Nice to see you again. Mitzi Wertheim; I'm with the Cebrowski Institute at the Naval Postgraduate School and I run the Energy Conversation.

I want to ask about gaming. I mean, the Navy has done wargaming for decades, and are you – as you think about how you're going to do this, are you going to start expanding gaming as a way to get people to think beyond first-, second- and third-order consequences?

MR. LYNN: Yes. In particular, in the Quadrennial Defense Review, we've got three types of activities that all involve wargame- and scenario-playing. One of the just kind of

conventional military scenarios, we've added a cybercomponent to those so that we understand what the implications of Georgia and other harbingers of what we think the future might bring.

Second, we have a red team that's led by Andy Marshall, the director of Net Assessment at the Pentagon, and Jim Mattis, who's the commander of Force Command, General Jim Mattis, and they are doing a red-team analysis of those same scenarios. And they have an even heavier emphasis on cyberscenarios.

And then we've asked some of our cyberexperts in the department to just think about some stand-alone cyberscenarios. So we're – we're taking the cyberthreat very seriously as one of the several focuses of the Quadrennial Defense Review, and we're trying to come at it from very angle.

Q: Good morning, Mr. Secretary. Max Cacas from Federal News Radio.

I'm wondering if you could expand on something you said, sir, that the – you said that the Defense secretary, Mr. Gates, is still refining some of his thoughts about where he wants to go with this. Could you expand on that a little bit? And also, do you anticipate a need for any sort of legislative help from Capitol Hill to get this – to get this done?

MR. LYNN: Well, yeah, as I said – the secretary is evaluating proposals. The Joint Staff is still working out the details of how this command would work and what the reporting relationships are. The – in terms of legislation, this is a subunified command of an existing unified command, so you wouldn't need legislation for that.

You would – you would need the commander of the Cyber Command, if we create that, would be subject to Senate confirmation, however. So Congress would be involved in that way. And of course, we would consult – we wouldn't do this in a vacuum; we will consult actively with Congress before we move forward on this.

MR. LEWIS: The fellow right in front.

Q: Al Pessin from VOA.

Can you give us some insight into U.S. offensive cyberoperations? You talked almost exclusively about defense. What is DOD doing to take this fight to U.S. adversaries around the world?

MR. LYNN: Well, I'm not going to really be able to go beyond the Aviation Week response, which is the emphasis of the – of the – setting up this subunified command is to unify all aspects of our cybercapabilities so that we're able to act in a – in a single fashion as – in a(n) appropriate military way with the appropriate controls and civilian oversight. And I really can't go beyond that kind of answer.

Okay. Any more?

MR. LEWIS: We have two more, and that'll be it. How about if we – we'll do – since Aviation Week got mentioned, we'll give you a second try.

Q: Thank you.

Companies like BAE Systems, for example, are working on developing systems for the non-expert so that they can take cyberattack to the tactical level. Is your area of interest in finally working that capability down to the company level, the battalion level?

MR. LYNN: Well, I think that the – our cybernetworks go all the way down to the company and the platoon and indeed the individual level as they go forward. So we – we certainly want to have all of the – the full suite of capabilities run up and down the force. So absolutely, yes.

MR. LEWIS: Okay. We had one in the middle there.

Q: Mr. Secretary, do you think that there's a – it appears to me that there's not – it's not as easy in the cyberworld to break out the demarcation between dot-mil, dot-gov and dot-com as it is in the conventional world. Do you think that that's progressing in some fashion that's making progress?

MR. LYNN: Well, I'm not quite sure; it's easy to break out the – who's on what network.

Q: Yeah, no, I get that. But I think there's a defense aspect to someone doing something in the cyberworld offensively in dot-com or dot-gov, and so it's a fairly porous relationship between those three, much more so than in other aspects of conventional warfare.

So it isn't – I know you were very clear to say that DOD is going to worry about, you know, dot-mil. But I think that there are – there is some shared responsibility for all three agencies across all three segments. And I'm wondering what your view on that is.

MR. LYNN: Well, no, that's absolutely right. And as – with regard to the dot-gov, I mean, the principal responsibility for the dot-gov networks remains with the Homeland Security department, and we – as we do with other domestic agencies, whether with – you know, with manmade disasters or natural disasters, we provide military support to civilian authorities. And in that context, we provide support to Homeland Security, try and help them with capabilities we might have that would help them accomplish their mission. But it's the Homeland Security department that's the lead agency.

With regard to the dot-com, it's the private sector that's the lead. And as – in answer to Tony Capaccio's question, I talked about the partnerships that we're developing and the exchange of information. But that's – the principal role of the Department of Defense is in that area, not in terms of actually going out and protecting dot-com.

MR. LEWIS: Okay. One more. And then let me – before we go to that question, let me make two requests. I'm fine. Can you hear me, everyone? I'll just yell.

First, given the size of the audience, when we get through with the questions – and we'll take a couple more – would you mind please remaining in your seat so that the deputy secretary can make his escape? (Laughter.) That would be – we would really appreciate it if you would do that.

The second thing, Marian (sp), I don't know if you want to stand up and talk about your event, but we're having another event tomorrow looking at NORTHCOM. It's at 10:00. Do you want to say anything?

MS. : Sure. It's a Military Strategy Forum event at 10 tomorrow, here. The breakfast reception starts at 9:30. It'll go on from 10:00 to noon with General Renuart speaking, and followed by the panel with – (inaudible, off mike) – experts on homeland security. And I'm sure cyber will also – (inaudible) – tomorrow.

MR. LEWIS: So General Renuart, NORTHCOM, Homeland, Defense.

MS. : And if you could RSVP on the CSIS Web site.

MR. LYNN: Yeah, 10:00. Thank you.

We had a question in the front.

Q: Thank you. Geoff Fein, Defense Daily. You talked about speed and how fast the response is going to have to be, but the acquisition process takes a long time. Are you going to have to reexamine how you acquire IT and, you know, maybe look for changes in the – DOD 5000 to do this?

MR. LYNN: We're certainly going to have to examine how we acquire IT and to make sure that we're in a position to acquire the tools and the kinds of software and the firewalls, the various things that get to the maneuver warfare I talked about. Whether that gets you to a 5000 rewrite, we're not there at this point. We're trying to figure out how to be agile within the existing authorities.

MR. LEWIS: Okay. Maybe one more from –

Q: Hi. Siobhan Gorman with The Wall Street Journal. Just one follow-up on a couple of the questions that have been asked. In terms of your statement saying that this isn't the militarization of cyberspace and that DOD is just providing support to agencies like Homeland Security, I'm just wondering, given that DOD sort of vastly outnumbered DHS – I mean, you were talking about numbers of 90,000; I know that not all those people are obviously working directly on cyberdefense –

MR. LYNN: Yeah, that's –

Q: – but how is it that you are going to kind of put forward this delicate balance? You were kind of saying that there would be a balance that would be struck, but how are you going to manage that level of support without kind of overtaking those efforts, given that DOD really is where the capability is?

MR. LYNN: Well, I mean, that's what I – that – that's where I was going with the – I – we – I think we do need to take the – take advantage of DOD's capabilities. We do need to do it in the way you suggest, in that we have to be conscious that DOD's role here is a supporting role. It's not a primary role.

And we – one of the reasons I think the president set up the 60-day review was to work on building the Homeland Security and the other domestic capabilities so that they will be able to fully absorb the responsibilities of protecting our – our U.S. domestic networks, protect the – particularly starting with the particularly starting with the dot-gov, and then work with industry on the key areas – finance, transportation, energy, communications.

But that role does fall to homeland security. The cybercoordinator that the president will set up will be coordinating – coordinating that effort. And I think that one of the principal outputs of that 60-day review will be a strengthening of domestic capabilities.

MR. LEWIS: Okay. Well, with that, let me remind you if you could just keep your seats for a minute. And second, could you join me in thanking –

(Applause.)

(END)