CENTER FOR
STRATEGIC AND INTERNATIONAL STUDIES (CSIS)

CSIS CYBERSECURITY POLICY DEBATE SERIES:
U.S. CYBERSECURITY POLICY AND THE ROLE OF U.S. CYBERCOM

WELCOME:
JOHN HAMRE,
PRESIDENT AND CEO,
CSIS

MODERATOR:
JAMES LEWIS,
DIRECTOR, TECHNOLOGY AND PUBLIC POLICY PROGRAM,
CSIS

SPEAKER:
GEN. KEITH ALEXANDER,
DIRECTOR, NATIONAL SECURITY AGENCY
COMMANDER, U.S. CYBER COMMAND

THURSDAY, JUNE 3, 2010
9:30 A.M.
WASHINGTON, D.C.

Transcript by
Federal News Service
Washington, D.C.

JOHN HAMRE: Good morning, everybody. Welcome, we're glad you're here. My name is John Hamre. I'm the president at CSIS. Gen. Alexander, he had to endure the travails of Washington traffic and I think – he said as he walked up, he said, well, there must have been a distributed denial-of-service attack on the lights in Washington – (laughter) – because I think he hit every darn red light that he could find. But we're so glad that he could come.

This is a session – I've been bugging Gen. Alexander to come here for, I think, about seven months. When it first became clear he was going to be the head of the new Cyber Command, it wasn't clear to some members of Congress. (Laughter.) It just took a hell of a lot longer than it should have. It was obvious that he was the right man at the right time, a time when we very much need this.

Now, this is going to be far more traumatic, I think, for NSA than it's going to be for the nation to have a Cyber Command because this is an agency that – well, who was it – somebody this morning said NSA used to – (inaudible) – that the NSA said, "no such agency," it used to stand for.

And of course, this is an agency that does so many crucial things for the country but it has to, by necessity, be in a reserved role in terms of public acknowledgment. And now, all of a sudden, to be thrust into the limelight on what's probably the largest and most public security issue we face is going to be a very wrenching thing for an agency – no small measure because we do not have the kind of consensus, the national consensus that we need at this crucial hour.

For the last several years, we've had a great debate in this country that has not resolved itself in the right way. We have two contending priorities. We want the government to protect us and Americans want to be protected from their government. These are two things that have been with us for 250 years. And we worked that out. We had a working formula that resolved all of that.

But that consensus broke down badly in the last decade. And so we have Gen. Alexander walking into probably the most crucial job that we need to have done at a time when we don't have – we, the policy leaders, don't have consensus on how to manage this. This is going to be the great challenge. So fortunately, we have a man of his talent and in his experience that's going to help us. He not only has to build a new organization but he also has to help build the confidence and the consensus in the United States that we need this role. And it's a crucial role for the country.

So I'm very grateful, Gen. Alexander, that you would join this. This has been long in coming. You see the depth of interest in this topic. And rather than my delaying it, we look forward to hearing your words. And then I hope you'll give us the benefit also of sharing Q&A and Jim will take care of fielding those questions for you. So thank you for coming. (Applause.)

GEN. KEITH ALEXANDER: He must have been standing on something because this was way up there. Sir, thanks for that introduction, and thank you as well for your leadership and service to our nation not only at the Department of Defense but also here at the Center for Strategic and International Studies.

You helped spark the discussions on cyberspace issues in the 1990s under the Clinton administration. And with experts like Jim Lewis, CSIS is continuing to show leadership in this field. Indeed, CSIS's December 2008 report, "Securing Cyberspace for the 44th Presidency," served as a key thread of continuity across two administrations and really set the foundation for crafting this administration's strategy for cyber and security.

Thank you as well for the opportunity to speak here today, as this is my first public engagement since I've been promoted in assuming the command of U.S. Cyber Command. I am pleased to be here with all of you today and can think of no better place to talk about cyberspace and U.S. CYBERCOM than here at CSIS.

But before I talk about U.S. CYBERCOM and focus on the Defense Department, let me state upfront that cyber security is a team sport. And I see a lot of the team out here in the audience. We can't do this alone. Within the government, Howard Schmidt has the lead for coordinating the departments and agencies in our approach to cybersecurity.

He has done a superb job and has been great to work with. For the team at DHS, Phil Reitinger, Rear Adm. Mike Brown and others have been great partners on a set of very complex issues. All of us in government recognize that government cannot do this without the help of industry, academia and our allies. Securing cyberspace is a team sport and we are proud to be a member of that team. We look forward to growing the partnership as we collectively address how we should secure our networks.

Let me talk about our portion of the team and our roles and responsibilities. Two weeks ago, I was privileged to participate in the activation of U.S. Cyber Command – as Dr. Hamre said, a task long in the making and longer overdue. I think it was a brief confirmation process that we went through. That was a joke, I'm sorry. (Laughter.) No more jokes.

In 2005, the director of NSA was dual-hatted as the director of NSA and the commander of the Joint Functional Component Command-Net Warfare. The commander of the Defense Information Systems Agency was dual-hatted as commander of the Joint Task Force-Global Network Operations.

In late 2008, as a result of a serious intrusion into our classified networks, the secretary of defense decided to place the Joint Task Force-Global Network Ops under my operational control as the commander of the Joint Functional Component Command-Net Warfare, recognizing both the imperative for better synchronizing our offensive and defensive cybercapabilities as well as the need to leverage NSA's intelligence capabilities to support our understanding of the threat and the ability to respond to it.

Last June, the secretary of defense directed the standup of U.S. Cyber Command to further strengthen this model and streamline the command and control of our military's cybercapabilities. Since that time, we have been leaning forward and building an organization and a mission alignment that is more integrated, synchronized and effective in the support of our soldiers, sailors, airmen, Marines, Coast Guardsmen and civilians. On May 21st, that came together in the activation of U.S. Cyber Command.

We at Cyber Command are responsible day to day for directing the operations and defense of the Department of Defense information networks and for the systemic and adaptive planning, integration and synchronization of cyber-activities, and when directed under the authority of the president, the secretary of defense and the commander of U.S. STRATCOM, for conducting full-spectrum military cyberspace operation to ensure U.S. and allied freedom of action in cyberspace.

That is quite a mouthful. I have difficulty saying it. I'm an Army officer. Reading is difficult. (Laughter.) Partly, it means that U.S. Cyber Command will centralize command of military cyberspace operations, strengthen DOD cyberspace capabilities and integrate and bolster DOD cyber-expertise.

Deputy Secretary of Defense William Lynn explained our mission concisely last week: We will lead the day-to-day defense of all military networks, support military and counterterrorism missions and, under the leadership of Homeland Security, assist other government and civil authorities and industry partners. As Secretary Lynn put it, "The key part of Cyber Command is the linking of intelligence, offense and defense under one roof."

It's that simple, right? Well, actually, no. It's not so simple at all, and it certainly will not be easy. The easy and simple stuff was done long ago. We got the rest. We have an enormous challenge ahead of us as a nation, as a department and as a command. If I may, I'd like to sketch out some of our thinking on the interrelated set of issues that we call cyberspace and on how we hope to sort these issues, I hope, resolve some of more urgent-demand issues.

Cyberspace consists of vexingly complex systems that ship and store unimaginably vast amounts of data. By 2015, the number of network posts is expected to exceed the human population. As Harry Raduege knows, I'm doing my part to compete against that with 12 grandchildren – (laughter) – but it won't work.

Social networking and instant messaging accounts are exploding. By the end of 2010, The Radicati Group projects that there will be 2.2 billion social network accounts worldwide, and currently, 2.4 billion instant messaging accounts. By 2014, they project that there will be over 3.7 billion social networking accounts and over 3.5 billion instant messaging accounts.

In 1996, there were 16 million Internet users worldwide. Today, there are approximately 1.8 billion Internet users across the globe. In 2009, there were a total of 90 trillion e-mails sent. And in 2010, around 247 billion e-mails sent every day. Of those 247 billion e-mails, 200 billion were spam. You might ask how I know that. (Laughter.) I got all the spam ones in my home account. (Laughter.) I think we share those.

Geographically speaking, those e-mail uses are probably not where you think they are. Forty-seven percent are in Asia, 23 percent from Europe and only 14 percent from North America, and 16 percent from other locations around the globe. In a sense, we humans are tying together all of the libraries on our planet and making them accessible from everywhere instantly. The data in that common library of humanity increasingly form the basis of our economic wealth and contribute to our quality of life. Tremendous opportunities for the future and tremendous vulnerabilities, our data must be protected.

No one here or anywhere else would consent to having all their personal and family information stored in a place where any random stranger could rummage through it. No business or nonprofit enterprise and certainly no nation could long afford to leave its trade secrets, donor lists or diplomatic bargaining positions lying around exposed.

And yet, that is what, in essence, is happening more and more as the ways we use to protect our personal enterprise and national security data are compromised by carelessness, poor design and subterfuge. We now live in a world where a nation's security depends in no small part on the security awareness and practices of our agencies, firms, suppliers, schools, friends, neighbors, relatives and, well, all of us.

Cyberspace has become a critical enabler for all elements of national and military power. As President Obama's national security strategy states, our digital infrastructure therefore is a strategic national asset. And protecting it, while safeguarding privacy and civil liberties, is a national security priority. The comprehensive National Cyber Initiative, which has been forged and implemented under two administrations now is our guide for doing this.

Today, our nation's interests are in jeopardy. The technologic convergence of automated data processing and telecommunications has boosted productivity and opportunity but it has also introduced tremendous vulnerabilities and created new challenges. It is not alarmist to say that the weakest link in our security can seriously impact our ability to operate securely and with confidence in cyberspace.

America's very wealth and strength make it a target in cyberspace. And one of the pillars of that strength, our military, is at risk, perhaps to an even greater degree. Our military depends on its network for command and control, communications, intelligence, operations and logistics. We in the Department of Defense have more than 7 million machines to protect, linked in 15,000 networks with 21 satellite gateways and 20,000 commercial circuits composed of countless devices and components.

National and military information infrastructures, moreover, are increasingly intertwined. They include the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries. That infrastructure is sophisticated and robust, but it also has its weak points. DOD systems are probed by unauthorized users approximately 250,000 times an hour, over 6 million times a day.

And while our frontline defenses are up to this challenge, we still have to devote too much of our time and resources to dealing with relatively mundane problems such as poorly engineered software, missing patches and poor configuration. You are all familiar with the general outline of the threats to network security from a growing array of foreign actors, terrorists, criminal groups and individual hackers.

Indeed, these outlines are no secret to analysts inside and outside government and are being treated and studied by industry efforts like Verizon's Business Risk Team. In the data breaches that Verizon investigated last year – and remember, these were only reported cases, not all breaches – they found that criminal organizations, often using custom-built malware, are able to breach virtually every single organization they choose.

A relatively handful – a relative handful of such attacks accounted for the vast preponderance of the 285 million records that the Verizon investigators determined to be compromised. And the main limitations on the abilities of these criminal organizations were time and resources. They simply did not have the time and the wherewithal to breach all the high-value targets they could have. And thus, they apparently concentrated on what they deemed the most profitable ones.

Those are just the criminal organizations. We should assume that foreign government actors in cyberspace have both considerably more resources and even more worrisome, motivations, than cybercriminals. In short, we face a dangerous combination of known and unknown vulnerabilities, strong adversary capabilities and weak situational awareness.

The trends seem to be evolving in other ways that should also give us concern. A decade ago, network penetrations seemed targeted mostly at exploiting data. In the last few years, we saw the bar of conduct lowered for computer network attacks. In Estonia, in 2007 and in Georgia, in 2008, distributed denial-of-service attacks impeded government functions.

And as I told Dr. Hamre, I think they also delayed me getting here. (Laughter.) Now, there are hints that some penetrations are targeting systems for remote sabotage. Let me explain. Estonia and Georgia were distributed denial-of-service attacks. Once these attacks stopped, the information systems were able to continue on with their job.

But the potential for sabotage and destruction is now possible and something we must treat very seriously. And these threats are serious. To deal with them will require common vision, unity of effort and a commitment of dedicated resources. Our Department of Defense must be able to operate freely and defend its resources in cyberspace.

We will do this as we do it in the traditional military domains of land, sea, air and space. But cyberspace is unique. It is a man-made domain. It is also an increasingly contested domain. That makes everything even tougher. Our job in U.S. Cyber Command is to assure the right information gets to the right user at the right time at the right level of protection.

U.S. Cyber Command enables the Defense Department to better operate and protect our DOD information networks and remains the focal point for military cyberspace operations in

collaboration with other components of the U.S. government. Its contribution represents a substantial share of what the department offers as part of a full-government approach to deter, detect and defend against emerging threats to our nation in cyberspace.

How will we do our job? As I mentioned earlier, we consolidated two already existing staffs, the Joint Functional Component Command for Net Warfare and the Joint Taskforce Global Network Operations. Recently, we established a single, coherent Cyber Joint Operations Center, bringing together the capabilities of these two staffs.

And we are currently executing command-and-control of our information networks from Fort Meade. U.S. Cyber Command is collocated with the National Security Agency, which it is also my privilege to lead. NSA's capabilities, and more importantly, its people in the intelligence and information-assurance fields are unsurpassed.

This intellectual and technological capital is critical to the success of the entire U.S. government efforts in cyberspace. U.S. Cyber Command is a military command that falls under Title 10, but its business relies on the success of net-speed intelligence, which is why collocating the command with NSA was not only wise, but an imperative.

I know that some have concerns about intelligence community involvement in securing the nation's cyber infrastructure. Those concerns are valid, which is why the professionals at the National Security Agency have robust and rigorous procedures to minimize the effects of intelligence activities upon U.S. persons.

NSA also has an experienced and energetic oversight, both internally and from the Department of Justice, the FISA court and from Congress. This explains why collocation of Cyber Command with those same professionals is perhaps the best way to ensure the transparency of operations that can affect U.S. persons' data and the protection of privacy and civil liberties as our military operates in cyberspace.

As of May 21st, U.S. Cyber Command also gained service elements to be boots on the ground in support of its mission. These include the Army Forces Cyber Command, the Marine Forces Cyber Command, the 24th Air Force and the Navy's 10th Fleet, Fleet Cyber Command under Vice Admiral Barry McCullough, who I understand spoke to you just a few months ago.

Well, technology is part of the solution, of course, but the key is people and we have superb people, both at NSA and at U.S. Cyber Command. But one of our greatest challenges will be successfully recruiting, training and retaining our cyber cadre to ensure that we can sustain our ability to operate effectively in cyberspace for the long term.

This is one of the key focus areas identified in the recent Quadrennial Defense Review, the need to develop greater cyber expertise. The QDR identified three other key imperatives for operating effectively in cyberspace. One, we must develop a comprehensive approach to DOD operations in cyberspace. Two, we must centralize command of cyber operations and three, finally, we must enhance partnerships with other agencies in the government.

This last point merits particular elaboration. Our mission at Cyber Command includes not only the defense of our military networks, but also a role in guarding our nation's defense-industrial base. More than 90 percent of our military's energy is generated and distributed by the private sector and more than 80 percent of our logistics are transported by private companies.

Mission-critical systems are designed, built and often maintained by defense contractors. The military's networks are not neatly bounded by those ending in the .mil. We rely on private-sector networks and capabilities, hence ensuring that those partners and allies' networks are secured is a key concern because the flow of information crossing these networks is significant and sensitive.

Our adversaries will find our weakest link and exploit it, whether it is public or privately owned and operated. That being said, any efforts to secure DOD mission-critical networks will be carefully designed to avoid providing preferential treatment to any particular private-sector company. Perhaps most importantly, this is an action that we need to do in partnership with DHS.

At U.S. Cyber Command, we will approach these tasks by ensuring the right balance of integrated cyber and technical capabilities. We will pull together existing cyberspace resources to create better synergy and synchronization of warfighting effects to defend DOD's information networks. We are integrating defense, offense, operations and we'll leverage technical capabilities to provide coherent effects to strategic, operational and tactical commanders.

All of these steps support the armed services' ability to conduct high-tempo, effective operations while protecting command-and-control systems and cyber infrastructure. In closing, I'd like to leave you with some thoughts on how I think we can translate these imperatives into mission success to operate effectively in cyberspace and how we can achieve these effects that we want.

We must first understand our networks and build an effective cyber-situational awareness in real time through a common, shareable operating picture. We must share indications in warning threat data at Net speed among and between the various operating domains. We must synchronize command-and-control of integrated defensive and offensive capabilities, also at Net speed.

We must leverage all tools of national power to ensure that America and other nations can gain the benefits of free movement in cyberspace, continue to conduct international engagement and diplomacy efforts to improve global governments of this domain, review military doctrine and actions to ensure they're appropriate and effective and consider economic policy tools with the involvement of intelligence and law enforcement agencies to dissuade those who seek to exploit cyberspace for illicit gain.

To achieve these efforts, we must recruit, educate, train, invest in and retain a cadre of cyber experts who will be conducting seamlessly interoperability – seamless interoperability across the full spectrum of network operations. Finally, we must be able to operate and adapt to situations at net speed, leveraging technology for automated, autonomous decision-making.

Together, NSA and U.S. Cyber Command will be the intersection of military, intelligence and information-assurance capabilities vital to the nation's comprehensive cybersecurity strategy. We will perform this mission with your trust and confidence, but we will only succeed by working as part of a coherent team.

We will partner with all departments and agencies. We will actively engage all branches of government. And we will exercise our powers and responsibilities under laws and ways designed to ensure that we are truly protecting, not infringing, the privacy and civil liberties of our fellow citizens.

I appreciate the opportunity to share my thoughts with you today. Cybersecurity is among the most current and future challenges DOD and our nation faces. Securing our networks is not just a DOD issue. It is a national security issue with implications for all instruments of national power.

The Department of Defense, through U.S. Cyber Command, will do its part to protect our great nation from elements wishing to do us harm in cyberspace. As I said at the beginning, it is a privilege and honor to be a member of our cyber team. And now, it's time for me to listen to your questions and concerns and I hope to broaden the dialogue that you at CSIS have promoted on cyberspace issues. I look forward to the interchange and I thank you very much, again, for your attention. (Applause.)

MR. LEWIS: Great, well, thank you, Gen. Alexander and congratulations on four-star. If I could ask when people ask raise their questions, could you do me two favors? Could you identify yourself when you ask them and could you keep the questions brief so we can respect the general's schedule? He does have a few other things to do. With that, we had one over right in the front row, there.

Q: (Inaudible, off mike.)

MR. LEWIS: Hang on. You get a free mike out of this. (Laughter.)

Q: One of the questions I keep getting asked is how do you streamline your – obtaining permission for cyberattack in time for it to be tactically relevant, particularly against stateless opponents?

GEN. ALEXANDER: That's a – that is a difficult issue. I think the question, I think everybody heard, is how do you streamline your counterattacks against CNA attackers, especially if they're stateless? I think I would enlarge it to say and if you can't attribute it, how do you do that?

And I think what we have to establish are clear rules of engagement that say what we can stop. Now, there are things that we can stop at the boundary like an intrusion-prevention system that's one part of that strategy. But in the future, that may not be specific. So what the department is looking at are what are the standing rules of engagement that we have?

Do those comport with the laws, the responsibilities that we have? Can we clearly articulate those so that people know and expect what will happen? And I think we have to look at it in two different venues, what we're doing here in peacetime and what we need to do in wartime to support those units that are in combat. And how do we ensure that the combat commanders have the command and control they need?

If you think about it, this is the Internet, the digital Internet, is now the command and control system which, in the past, was our old push-to-talk radio. And when somebody would jam it, you would try to work through it. Now how are we going to do that in cyberspace? And the answer is, I believe, by working through a set of standing rules of engagement that we'll have and our forces will have. And we've yet to do that. That's something that we have to take on.

Q: But do you see two sets of rules, a war concept and a peace concept?

GEN. ALEXANDER: I do. I think that they may all be in one set, but those things that you do in wartime, I think, are going to be different than what you do in peacetime? And I had an opportunity in the hearing – I say this with some level of humor – was asked this specific question by Sen. Levin when we came up with three different menus.

So how would Cyber Command act when we're at war with another country, where both combatants are in one country and you could attribute the attack to your aggressor, your adversary, and you'd say: Now I know I'm going to do these and I'm under one set of rules of engagement. Now what happens – that was case one.

Case two is, what happens when the adversary uses a neutral country to bounce their attack through? And that is a different set. And it's not unlike warfare, where you have two – you have armed conflict going in one state and somebody attacks from a neutral state in. There are laws of land warfare that deal with that. We now have to look at that in light of cyberspace.

And then the third is, what happens when it's the United States that's under attack? What are the rules for that and how do we go through the threat conditions and stuff to mitigate or defeat that threat? So those were the three conditions and we talked about each one in a different case.

And as you think about those, each one of those are going to have different standing rules of engagement. And now, what we don't have is the precision in those standing rules of engagement, yet, that we need. And we're working through those with the USD policy and up through the deputies' committees for the administration.

MR. LEWIS: I think we had Harry and then the gentleman in brown. Harry, do you want to?

Q: Good morning, sir. Harry Raduege from Deloitte. Many of us have worked on situational awareness for many years – common operational pictures and such. And during your comments, you mentioned that situational awareness is an area that definitely needs to be

improved. I wonder if you couldn't just briefly describe, perhaps, where we are now with situational awareness and the areas that you'd like to see improved in the future.

GEN. ALEXANDER: Well, I think, in a nutshell, the hard part is – and I can give you an analogy here, so I'll use the National Training Center. In the National Training Center, one of the things that they teach our land forces is how to see the battlefield and how to react to different situations. And getting the picture for the battalion and brigade commander, as you know, is a very necessary part of how they're going to conduct their campaign against an adversary in a very quick battle – battalion-on-battalion, brigade-on-brigade – where fights may only last four to six hours.

So understanding where your adversary's trying to go, where his reconnaissance goes, where his leading forces go and all that, is some of the stuff that we do at the National Training Center. Now let's put it in cyberspace. We have no situational awareness. It's very limited. Often times, our situational awareness is, indeed, forensics, which means that something has happened. We are now responding to that and we're saying, okay, something got through. How do you see your network?

And as you know, as the former director of the Defense Information Systems Agency – a great agency – as you looked at that and you tried to look at all your networks, you didn't have real-time situational awareness of those 7 million machines and all your networks. And the consequence of that is, it was almost policing up after the fact versus mitigating it in real time. So the requirement, from my perspective: We need real-time situational awareness in our networks, to see where something bad is happening and to take action there at that time.

That is both a coordination issue amongst the services and agencies and a situational awareness issue. We do not have a COP, a common operating picture, for our networks. We need to get there. We need to build that. And I think many an industry would say, yep, we're working towards that. But we don't have that with the breadth that we need. Now, if you take that to Iraq and Afghanistan, you would find the same things. And so we need to fix both. I would focus first on the warfighting ones and then fix the second one, the global one, second.

MR. LEWIS: Let's get one on the other side of the room here. Yeah, go ahead.

Q: Good morning. My name is Scott Matthews. I'm with the office of technology at Department of Commerce. And the question I have is regarding Russia's proposal, with significant support in the U.N. General Assembly, for a cyberwarfare arms limitation treaty. And the question is whether you think something like that is possible. The other part of their proposal is to create, basically, sovereignty on the Net. And how would that – do you think that can work? And how would that impact your functions?

GEN. ALEXANDER: Let me take that in two parts: yes, no, no. (Laughter.) Let me elaborate, if I could. I do think that we have to establish the rules and I think what Russia's put forward is, perhaps, the starting point for international debate – not at my level, but at levels above me. And I think when they put that on the table, I think the secretary of defense, the secretary of state, the administration would take those, carefully consider those and say: Now,

what's the counterproposal from the United States, from China, from Russia, from Europe, from the Middle East? How do we put that on the table? And I think we do have to establish that in the lanes of the road.

With respect to sovereignty, that's much more complicated. And the reason is, well, look at our businesses as an example. They are multinational in nature. And as a consequence, working with business and industry – industry and business working with government – we have opened up a set of vectors that don't easily drop to geographic nation-state boundaries.

So I think the first may be the way to helping the second, the first part of your question. And I do think it's something that we should and probably will carefully consider. You know, I think those are the kinds of things that need to be put on the table, talked through and start out as a – call it version 1.0.

MR. LEWIS: Gentleman in the second row, please.

GEN. ALEXANDER: Randy, thanks for the call.

Q: General, Randy Fort, Raytheon. Congratulations on your promotion and thank you for your service. In your remarks, you talked about one of your – on your to-do list, discouraging malevolent or bad behavior. Another word for that might be deterrence.

And so I was wondering, since deterrence was one of the issues specified under the Comprehensive National Cybersecurity Initiative articulated in the previous administration – and that issue has continued to receive some attention – I just wondered, what are your thoughts for the potential of deterring the kinds of malevolent behaviors you talked about on the Web? Thanks.

GEN. ALEXANDER: Yeah, I used discourage because I couldn't pronounce the other word. You know, I had to break it down into different parts. I do think that deterrence – I think, let's go back to the previous question. If nation-states agree on what we're going to do to deter malicious actors in cyberspace, that will go a long ways to do this. In this case, it would be the Cyber Investigative Joint Task Force, the FBI's thing, that would actually take for within – the domestic capability's ours, as you well know.

They have a great capability. But it's not good enough for what we need. And I think there were some statistics last year that came out that said the amount of money being made in cyberspace has eclipsed the drug trade. And when you think about that, you could say: Well, good news. The drug trade is down. I don't think that's true. (Laughter.)

I think it's just the opposite. As a consequence, I think – putting it from a nation's perspective, what's on those networks that we've got to secure? Well, it's our intellectual property. It's the future of our country. It's the future of our industry. It's what going to – it will make up the future wealth of this nation. We've got to protect it.

And so I think establishing those rules of the road in cyberspace are going to be key. I think that's not a CYBERCOM or a Defense Department, per se, responsibility. We may play a part in it, but I think that's really going to be State, Justice and the administration. And we have a supporting role, a technical role. But I do think that laying out those rules and then going after those cyberactors – who can come from any place in the world, bounce through any place in the world and attack anyone with virtual impunity – are the ones that we have to policy up first. And it's a huge issue.

MR. LEWIS: We have one all the way in the back, there. Go ahead.

Q: Hi, good morning, General. And again, congratulations on your fourth star. Charles Dobb, Nisrab (ph). Some of the adversaries have been working on IPv6 level architecture attacks. Since the United States runs on IPv4, do you see some issues in converting over to IPv6, or are we going to look at a hybrid system to do next-generation cyberwarfare? Or do you see that as something that's already underway by multiple agencies?

GEN. ALEXANDER: I think there's a lot of folks looking at the transition from IPv4 to 6. I think it's something that we will have to do at some point, the question of security. You've hit all the key points. You know, it is kind of interesting. When you asked that, though, I can remember – somebody, we were trying to explain why we aren't at IPv6 in some of our capabilities and why we're at IPv4. And they said, why don't you have a middle road – why don't you go to IPv5? (Laughter.)

And then you thought, okay, so – so I'm not going to answer it that way, although on average, that's probably where you want to be. It doesn't exist. So I do think it's something that we're going to work our way through. I think you can see, technically, we're going to have to make those moves there. The number of addresses and things like that are key and we've got to come up with some of that. I'm not sure, and you probably are as aware as I am. There's a lot of debate. Do we take a step beyond that? What's that step going to be?

I think that's still open for discussion, but clearly you're going to have to take some of the benefits of IPv6, the addressing and other things. Look at – you know, I admitted that I have an iPad. And when you start to think about the tremendous capabilities that you have out there and you think about all these tools – your iPhones and all these things that are coming out – the computing on the edge is growing huge. We're going to have to account for that. And I think that's going to drive us down that road. I just don't know where it's going to end up.

MR. LEWIS: We had a lady over on the other side of the room.

Q: Good morning, sir. Kat Hollis, Institute for Defense Analysis. I have a question and I think it's pretty inherent. And it's been touched on a little bit. There's a vulnerability in cyber that I think we kind of ignore, which comes along with all the social engineering posed by our allies, our non-allies, other countries in the world.

Nation-states with little or no division between academia, industry and government, students raised with the goal of promoting their government's roles – there's little or no

repercussion for them. In fact, it's looked at in terms of, probably, a boon to their academic endeavors or their industrial endeavors if they can show ways that either they can get into, how they can compromise, how they can gain access into our networks, international networks – whether they're government or whether they're industry.

My concern is, how is – is Cyber Command, along with the other agencies, along with industry in the United States actually going to address this? Because I think, as we look in the future, that's where our real threat lies. These are people brought up in how to do what we're trying to learn how to do.

GEN. ALEXANDER: I think it goes back to the commerce issue that was asked earlier. I think the way to address that is by establishing the rules of the road. It's going to take all countries to get together and fix that. And when all countries can come up and agree, this is going to be the way we're going to operate and the way we're going to defend and the way we're going to do this – and we all agree to it – that will go a long way towards getting there.

And the key will be, how do we ensure that we all enforce it equally? That's going to be the hard part. And I think we're going to start walking down that road. That is not a U.S. CYBERCOM lead, as I stated earlier. I think that's going to be State, the administration and others. I think it's an international issue that has to be addressed and put on the table.

MR. LEWIS: We had someone in the second row, here.

GEN. ALEXANDER: A whole row of them.

Q: Siobhan Gorman with The Wall Street Journal. Thank you for doing this, sir. I had a follow-up on the situational awareness question. I was wondering what your role is in developing better situational awareness inside the U.S., sort of, nationally. And in addition to that, what is the government's, sort of, role, broadly, in terms of ensuring privacy protection as it tries to get a better handle on the problem?

GEN. ALEXANDER: Okay, well, a couple parts. Let me handle, first, my role with respect to the military networks and how we get situational awareness there. In a war zone, as I said, we gave three cases – in a war zone, the commander has to have confidence in his command-and-control system. Increasingly, our intelligence, our operations, our weapons platforms are all being brought together in cyberspace. We have to have confidence that, that space is secure.

And whoever is running that space for that commander in that area has to know that, that's secure. You can't afford to lose it. Tremendous vulnerabilities. So my responsibility, in that regard, is to help articulate the requirements in a wartime effort, and then if you think about the Defense Department networks globally, in the Defense Department's networks. That's my role.

If you look at the rest of the government, that's where Phil Reitinger and his folks are going to come in and say, how do I, now, help the other government departments and agencies

see their networks so that they can operate and defend those, just as the military will defend its? Our responsibility is to assist them, if they ask for it – request for assistance, request for technical assistance. We'll provide that assistance.

I think, from a national perspective, if we come up with a situational awareness tool – call it X – that we should have each other department pay to have X developed for them, too. Perhaps we could all use it – Microsoft Office, or something like that. I think that's the way to go through it.

Now, your third question, third part of that – civil liberties and privacy. I think the key in this is oversight. Now, this is really a tough issue when you think about civil liberties and privacy when you're talking about classified information and areas. And so the way we've set up the oversight on that is by having a set of oversight mechanisms by all branches of the government. Government, the court system and Congress all need to play a part in that and know that the actions that we're taking comport with law and protect the civil liberties and privacy of our people.

Now, there issues that you get into that – and you know, you can take it from a domestic side. So what's the FBI do and what do we do with a Foreign Intelligence Surveillance Act court? Both of those now get into classified areas, with oversight. And so I think we do that very well. The hard part is, we can't go out and tell everybody exactly what we did or we give up a capability that maybe extremely useful in protecting our country and our allies. And so that's the real – what I see as the two things that we balance.

And so I do spend a lot of time with the court and with Congress explaining exactly what we're doing, where we have issues, where there needs to be change, what we can and cannot do. And we put that up to the court and we get things back from the court. I think it is growing and getting better. We spend a lot of time on that. The hard part: We can't tell everybody what we're doing. It will be analogous to you explaining how you defended your system – your computer system.

You say, I'm defending my computer system using the following steps: one, two, three, four. The adversary will say, thank you, one, two, three, four, now I know how to get around it, and within a day, they're through. That's the problem that we face. And so I think the real key to the issue – how do we build the confidence that we're doing it right with the American people, with Congress and everybody else?

That's going to be the hard part. You play a key role in that. How do we explain it without giving up things that would cause us to have an attack or something go through while we concurrently protect our civil liberties and privacy? You know, I have four daughters, and, as we said, 12 grandchildren. And my daughters are huge users of this area and space, and they like their civil liberties and privacy, too. And we want to ensure that they have that. That's one of the key foundations that this nation was built on and that we take an oath to protect. And we take that very seriously.

MR. LEWIS: You know, I'm cognizant of the general's time and he's been very generous. So maybe two more questions – do you think that will work? Okay. How about if we get Arnaud there – I'll have to do an in-house question.

GEN. ALEXANDER: I think we can go about 10 more minutes.

Q: Arnaud de Borchgrave, CSIS, General. About 15 years ago, a great deal was written about the threat of cyberwarfare, cyberterrorism, the Marsh Commission. A monograph was produced by CSIS. I wonder why it took 15 years to stand up your command? (Laughter.)

GEN. ALEXANDER: Next question? (Laughter.) I think part of it had to do with, they had to teach me to read along the way. (Laughter.) And so that takes some time. Well, you know, that's a tough question to answer. One, was the department ready to stand it up? And how did we get there along the way?

It is interesting to look at this, and I do think it merits a more serious part of the answer. It's not like this was a step function in getting to U.S. Cyber Command, that the 21st, we said, no Cyber Command, no cyber – boom – we're here. If you go back to 2002, when you saw the department wrestling with, how were we going to do this, what we did is, we said, well first, which combatant command is going to have the responsibility?

We looked at that and went to Space Com, went to U.S. STRATCOM. STRATCOM said, so how am I going to do this? I need technical expertise. Who has technical expertise? They picked DSA, because then, General, were you there at that time? You see, Gen. Raduege was there. They gave him the global network ops – the defend-and-operate mission.

And then they said, now who can help with the offense? And they looked at NSA. And they dual-hatted both and then the rest is as I explained. But it takes time to evolve it, so it's not something we just jumped into. And I think it's a well-thought-out approach. And we are one step further along. And I think it's going pretty good.

MR. LEWIS: The lady in the center there – is that Kate? Hi, Kate.

Q: Hi, Kate Martin from the Center for National Security Studies, and I wanted to thank you, General, for your commitment to protecting civil liberties and privacy and your recognition of the importance of oversight by the court and the Congress, and acknowledge that the problem of protecting national security classified information is very difficult and important in this field, but ask you whether, nevertheless – in the last administration, I think lots of members of Congress, as well as those of us in the civil liberties community, concluded that, in fact, the intelligence capabilities were illegally trained on U.S. citizens.

And so the question becomes, despite those oversight mechanisms, how to prevent that from happening again, and whether or not you plan to undertake an initiative to look at the possibility of greater public transparency, given the necessity for national security secrecy in this field, in order to help build the public confidence that you referred to.

GEN. ALEXANDER: That's an easy question, and I'm going to turn it over to – no. (Laughter.) First, you made some statements that I don't agree 100 percent with, so I'm going to just put it back in my words, if I could. Illegal versus the constitutional Article I, Article II, Article III. Now, I'm not a lawyer. I just admitted that I just learned to read, so I'm not a lawyer.

So what are the rules of the three branches of the government and how do we do that? And what are the roles and responsibilities for the president to do his job, what are the roles for Congress and what are the roles for the court, are articulated in our Constitution. And what we have is a constitutional issue that was put down on the table. If you take 9/11, a tragic even for our country, the question is, how do we ensure that we don't have another terrorist attack and we don't give up our civil liberties and privacy?

Both of those are national objectives that we want to achieve, and when you look at that, are ones that we're trying to achieve. So I think what I can do is jump forward – it's hard for me to jump backwards, because I came in, in the middle of the last debate – and say, here's my opinion, the way to do this in the future: transparency at the classified level between Congress, the court and the administration on what we're doing so that all three agree 100 percent that this is the right way.

And I think that's the first and the most important step that we have, and I think we're doing that. We spend a lot of time with the court, with Congress and the administration, with the oversight committees, to ensure they know what we're doing, why are we doing it, and debate it there in a classified setting, and then with the court, go forward with the court and say what we're trying to do.

I think the American people should be – would be very pleased to know the way we're doing it. In fact, some would say, why does it take you so long? And I think the answer is, these are tough issues. You know, we have a lot of lawyers at NSA and in the nation – all good people, I'm sure. (Laughter.) You know, if we divided the room in half and put half the lawyers on one side and half on the other, we could debate this issue until we all go to sleep. And so the issue, I think, that we have – the one that we really face; the one that you're driving at – is where our country wants to be.

We want to protect – some say the Constitution is not a suicide pact, and I agree, but it's also not something that we're just going to throw out our civil liberties and privacy. We were built on that. that's how our country was built. We want to ensure that we do our part to it. My responsibility, as the director of NSA, is to ensure that what we do comports with law. And so every action that we take, we have legal reviews of it all the way up and down.

And as I said, when you look at that, there are a lot of legal reviews that go into this, many of which are classified for great reasons. Bottom line, I think we're doing this right. doesn't mean that we won't make a mistake. But from my perspective, I could tell you that we spend an awful lot of time ensuring that we're doing it, both to protect the country and everything that we can on that side and to protect civil liberties and privacy. And I'll tell you, I sleep good at night because of that.

MR. LEWIS: We started this series – AT&T has helped us to underwrite it and helped us support it – and we started this series in September of 2009 with Deputy Secretary Lynn, who was supposed to announce the creation of Cyber Command here. And I'm really grateful that we finally, some time later, got the results. I think that was a tremendous speech. Thank you very much for taking these questions, which were all difficult and good. And if you could join me in a round of applause. (Applause.)

(END)