Center for Strategic and International Studies

Military Strategy Forum: Admiral Michelle J. Howard on the Cyber Cold War

Speaker:
Admiral Michelle J. Howard,
Vice Chief of Naval Operations,
United States Navy

Moderator:
Dr. Kathleen H. Hicks
Senior Vice President, Henry A. Kissinger Chair, and
Director, International Security Program, CSIS

Location: CSIS, Washington, D.C.

Time: 9:00 a.m. EDT
Date: Friday, September 25, 2015

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

KATHLEEN H. HICKS: Perhaps you're here to see Admiral Howard, who's the vice CNO, and I'm going to give a quick introduction and turn the floor over to her. She does have a hard stop, so we're going to do a little less Q&A, probably, today than we normally do. But I promise I will take it from my time and not your time.

Admiral Howard is a 1982 graduate of the U.S. Naval Academy. She, early in her career, was awarded the Secretary of Navy-Navy League Captain Winifred Collins Award, given to one woman officer a year for outstanding leadership. She's had a series of command – command positions – excuse me. As commander of USS Rushmore in March of 1999, she became the first African-American woman to command a ship in the U.S. Navy. In 2009 she deployed to the CENTCOM theater, where she commanded Task Force 151, the multinational counterpiracy effort, and Task Force 51, expeditionary forces. And in 2010, she was the Maritime Task Force commander for BALTOPS under 6th Fleet. She has served in a variety of positions on the OPNAV staff and in Joint Staff, where I first met her, and of course now serves as the 38th vice chief of naval operations.

She's here to speak particularly this morning about cyber, which is ever timely. And so, Admiral Howard, the floor is yours. Thank you.

ADMIRAL MICHELLE J. HOWARD: Thank you, Kathleen. Thanks for the kind introduction. (Applause.)

Well, thanks for your time today. I have been proselytizing on cyber for about three years, and literally in the last 13 months have spoken probably over 200 times on this topic to the public, whether it's a Chamber of Commerce or a policy forum, strategy forum, industry day forum, or just high school students.

So there's a theory of the case that I've been working on. And what's great about the cyber domain is how it's not only connecting ideas, but it's connecting language and making things shorter and more concise. And I love the word "app," but in reality the word "app" is application. And so I'm going to talk to you today about what I think is the application of what we know and the lessons learned from the Cold War. And if you walk away unconvinced, please feel free to build your own app.

But for me, as I've had this conversation with different folks, from the public to my own sailors in all-hands call, it's helped me sharpen my thinking on where we are in this domain and what we need to do.

First slide.

So in order to talk about this metaphor of the Cold War and the cyber domain and what's going on, I find it useful just to sort of give a quick history recap. You know, it was actually George Orwell who, shortly after World War II, coined the term "Cold War" in a(n) article. And then that got picked up in another article by Walter Lippmann, and it was all about the atomic bomb – "You and the Atomic Bomb."

And during that same time frame, as the world continued to unfold and the United States was the sole power – atomic power – in ’47, nations got together and signed the North Atlantic Treaty. So April of ’47, we, as different world powers, are starting to get concerned about Soviet aggression. And then in August of – I’m sorry, August of that year, the Soviets explode their own first atomic weapon. And so now we’re into the nuclear age, with two countries with this capability.

After they did that, Harry S. Truman said, OK, the Soviets have an atomic bomb; I’m going to create a hydrogen bomb. And sure enough, shortly after that, in the Marshall Islands, we exploded a hydrogen bomb – 25 square miles of a plume and destruction that destroyed the Enewetak Atoll, and with enough energy that it could have destroyed half of Manhattan – (snaps fingers) – just like that. And that really is the start of where the world changed.

And it changed for all of us in this country. And we don’t have really, I think, a strong collective memory of this as the American public, but people started to build bomb shelters in their backyard. We started to have drills. We were into a new age and a new way of life, and there was a lot of fear associated with that.

Next slide.

There was not only a lot of fear, there was a lot of spying going on. The Russians were in us and around us – I’m sorry, the Soviets were around us and looking at us, and we were doing the same to them, trying to figure out and understand what the other person was doing. And at the same time, we start to codify this relationship. But the intensity of this fear and the potential of this weapon permeated. McCarthyism comes out. McCarthyism could be about communism, but it’s because of the communists one of the great powers had the bomb as well. In ’53 we convict the Rosenthals (sic; Rosenbergs) for selling nuclear secrets to the Soviets, and we execute them in Sing Sing Prison.

My service starts to come into this role of the Cold War with the launch of nuclear-powered submarines and the carrying of ballistic missiles. We start to settle into a more structured relationship. We stand up the Strategic Air Command in the ’50s, and that lasts until it becomes Strategic Command that we know today as a combatant commander.

All of this – this intensity – it was all up and front. We started to have a dialogue with the Soviet Union. We get into strategic arm(s) limitation talks. But what was interesting during this time frame, all of this – this tension between our nations and the angst in the public – for many of us, it was unplaying out in the conventional side. A lot of people say there were proxy wars between conventional forces. But I will tell you, as I came into the service, there was a lot of cat-and-mouse activity going on between our submarines, between our surface ships. It got to the point where we created an agreement called the Incidents at Sea to prevent unintentional miscommunication between U.S.

ships and Russian ships. What we didn't want to have happen is a conventional conflict or a(n) incident grow into something larger – grow into something like the use of the atomic weapon. And so we sort of settled into this, this is just the way life is.

Next slide.

So I come into this after – before the Berlin Wall falls. So I come into the service in '82. And as I started my life at sea, the Russians were still out there monitoring us all the time. We got quite used to it. We were trained as officers to expect that we would have this big fight at sea, and we were really very good at understanding the Russians – the Soviet Union, their tactics. And they were always watching us. Every time you went to sea, whether it was out of San Diego, San Francisco or Norfolk, there was somebody there with eyes on you. And so we believed, underneath this umbrella of nuclear deterrence, that there might be – possibly still be a conventional war fight with the Soviet Union.

Well, as an officer, our biggest threat was the – was the Soviet submarines. Now, during those days I was on a(n) ammunition ship. And you don't have any offensive capability on that kind of ship. We knew it would be up to the other folks in the battle group, folks who had – on the destroyers and cruisers with their sonar to find the submarines and basically protect us. But on the other hand, we came to the realization that, if you're on a ship like this with lots of ammo and you happen to take a torpedo, first of all, it would probably be OK because you wouldn't have to worry about the paperwork afterwards. (Laughter.) But in the end, if you took a torpedo and exploded, you'd probably wipe out the rest of the battle group if they were anywhere nearby.

And so we took this thought – this anti-submarine warfare role, where we had no offensive weapons – and said, hmm, we only have defensive measures on this ship at the tactical level. I can try and make the ship lighter. I can do zigzag patterns to make sure it's hard for a Soviet submarine to track me and figure out where to put a torpedo in the water. But one of the things we figured out was that if we spotted the Soviet submarine and could communicate that to the other folks in the battle group we'd have a better chance of surviving.

Well, we didn't have sonar, but we had lookouts. And so all of the folks across the waterfront who were on ammunition ships, we drilled our lookouts really hard – 17- and 18-year-olds. They were fantastic at spotting periscopes. They were the best.

And in those days there was a competition for who was the best as anti-submarine warfare. It got so that the folks on the ammunition ships were discovering more submarines with the lookouts and binoculars than the guys who had sonar. And finally the fleet commander said, I'm about to give the Battenberg Cup to an ammunition ship. So that made us feel good. But it also said that even though you just have defensive measures at the tactical level, if you're the best at your defensive measures, you can still contribute to the war fight. And that is a thought I want you to hang onto as I talk about where we are in this domain today.

And the other thought I want you to hang onto is when you look at the Cold War and how it unfolded, this threat of something that we couldn't see but knew had tremendous power, to how it affected the American public, to how it affected us in the conventional forces, what it said was everybody was in it, whether you were a civilian or military. Everybody played. Everyone played.

Next slide.

And that is the essence of what we're seeing in the cyber domain: everyone is in it, and everyone plays, and everyone has a role.

So the first thing I'd like to do is talk to you about: What does it mean, the cyber domain? And you got to think that it's this collection of space and satellites, fiber-optic cables and networks, and then this creation of a virtual world of bits and bytes. But I think one of the biggest differentiators about this domain as compared to the domain we live in every day is this concept of the speed of light. It's almost as if we've fallen into the fourth dimension – that we grew up in a three-dimensional world, and for me as a warfighter it's submarines, it's surface ships, cruisers and destroyers, it's airplanes, but when you look at this dimension it's the speed of light. And it makes a difference in who we are and how we think.

Have any of you ever read the book the "Wrinkle in Time"? Do any of you remember what it was about? Stand up. Come on up.

Q: I'm a reporter, so I – (laughter).

ADM. HOWARD: Don't embarrass me. Oh, turnabout is so fair play. (Laughter.) No, come on up. Come on up. I will not embarrass you, I promise.

Do you remember what it's about, time travel, the theme of –

Q: I do. I do.

ADM. HOWARD: Can you talk a little bit about what it's about?

Q: Not exactly, but – (laughter, laughs) – do I have to go sit down now? (Laughs, laughter.)

ADM. HOWARD: No, no, no. No. You're about to be rewarded for your courage.

Q: (Laughs.)

ADM. HOWARD: That's it, time travel.

Q: Time travel.

ADM. HOWARD: All right.

Q: A young woman goes through time, basically. It's easy.

ADM. HOWARD: A young woman goes through time. I think that's good enough. (Laughter.)

Q: OK.

ADM. HOWARD: Thank you for having the courage to come on up.

Q: Thanks, Admiral. (Laughs, applause.)

ADM. HOWARD: And I want you to remember how you just felt the next time you do an interview. (Laughter, laughs.)

So "Wrinkle in Time" is about time travel, and it's a way to introduce young folks to this concept of the fourth dimension and dimensionality. And we grew up in this physical world, and algebra says the shortest distance between two points is a straight line, when in reality the shortest distance between two points is to bring the two points together, or wrinkle – wrinkle the line. And then, if you're a time traveler, you just step through, right?

Well, what does that mean in this domain? Well, I first fell into the fourth dimension when I was a student at Leavenworth and I got my first computer. And it came in a Gateway box with cow markings on it. I wasn't sure what that was about. (Laughter.) And I – and this was '97 – and I set it up in my house, and it didn't work right. And so I called this 1-800 number, and there was this guy from India. And that's how long ago it was: he said he was from India. (Laughter.) And we're trying to work our way. He's talking to me and I'm trying to do things on this new thing. And he finally says, may I take control of your computer? And I go, well, sure. (Chuckles.) And he does. He's an Indian. I'm in Leavenworth, Kansas. And so from, like, two continents away he takes control of my computer and I start to see my cursor move. He is making things happen on my computer at the speed of light, halfway around the world. That is as close to time travel as we're going to get, probably, in our lifetimes.

But do we understand that we now have the power of time travel and the power of making physical effects in this world at the speed of light? That is a very powerful and innovative weapon, up there probably with a nuclear bomb. And we're all in it.

This domain is unbelievably crowded. When I grew up, I thought if I was going to have a conventional fight with the Soviets, it was going to be in the deep blue sea. I was going to see images coming over me on radar. It might be bears. It might be their destroyers and cruisers. But I would very cleanly and very simply know what was about

to happen. It was a world with a single enemy. It was simple. I'm not saying it wasn't unpredictable, but it was simple.

This is an urban fight domain. There are civilians in here. There's businesspeople in here. There's criminals in here, who are dominating this domain. There's vigilantes in here because it's unregulated. So when you think about ISIL and what they're doing in terms of communications, it was the hacker group Anonymous who finally, in April of – March of this year said, hey, we're going to start identifying ISIL accounts and we'll turn them over to Twitter. They identified 9,200 accounts that they thought were ISIL, and Twitter ended up shutting down 800. That's vigilantism.

I think about Aramco in 2012, one of the largest OPEC producing companies, in Saudi Arabia – 30,000 computers shut down in a single day. The employees don't have email, files, any way to communicate with each other. All with an attempt to disrupt oil production.

And so, when I talk to my sailors about this domain, I go, can you imagine being in a battle group and having all of your computers shut down in a single day? How would you operate? How would you fight the ship? How would you fight the enemy?

And clearly, there's political motivations going on. When you look at the Guardians of Peace and what North Korea did, people are using this domain. And I predict everything that we've seen unfold in the physical world we're eventually going to see unfold in this domain. The ones who seem to be getting there first are the criminals, but it's just – it's just a matter of time and imagination.

And there's great value to this domain. It's ideas connect, it's innovation, but there's also vulnerabilities. But it's right here, just the way for many of us nuclear weapons were right here for so long. And it's unfolding in a different way.

So when I look at how do my people understand where we are in this domain and where we are as warfighters, and I look at my sailors, I think about what they understand about this domain. You know, depending on who you talk to, we say Millenials, they're the largest generation in the country. They were born between 1980 and possibly the mid-2000s. But when you think about when the World Wide Web was born, in 1994, the Millenials don't know any other life, and so they don't have a fear of this domain. And so we're starting to see trust and confidence in this domain just the way we stopped really thinking about nuclear weapons. When I grew up, we actually got underneath the school desk and, you know, hid as a drill.

For my Navy, 83 percent of my sailors are Millenials, and 53 percent of my officer corps is Millenials. So how they think about this domain is very different than how I think about it.

Next slide.

And so I find that I have to talk to them about this domain in terms of the strategic level, the operational level and the tactical level. And what's interestingly enough, as this domain has unfolded, at the tactical level we are only giving these sailors and officers defensive weapons – just like I did on that ammunition ship. We talk to them about defending the networks, because arguably if we have offensive weapons they're being held at the strategic level, a lot like nuclear weapons – that if we're going to use a cyber offensive weapon, it's probably going to take the permission of the president to do that.

And that's interesting because that's where we started off with nuclear weapons. And yet, at some point, we went on this journey where we said, hey, this is a powerful weapon, we'll take it all the way down to the tactical level. And at some point in our history, we actually had nuclear weapons on the – on artillery in Europe. My Navy put nuclear weapons on depth charges. And then at some point somebody goes, hmm, tactical nuclear weapons, maybe not such a good idea. And we brought it all the way back up to the strategic level, with that kind of command-and-control and authorities being held at that level.

And so this will be interesting to see if we go on the same journey with cyber. Are we going to go all the way down to the tactical level release authority with offensive weapons, or are we going to keep it up at the strategic level? But for now, if you're a sailor, it's defensive. You defend your network. You do your patching. You look for intruders. But then it is the actual individual sailor that is also potentially my vulnerability.

So when I talk to my sailors, I do take them back to the Cold War. And I'll go, hey, did any of you ever see a submarine movie when you were growing up? And they'll go, yeah. And then I go, so, in all these great submarine movies, there's always one submarine against another submarine, and they know they're both there, and they're quiet and they're listening – Americans against the Soviets. And then what happens? Any takers?

Q: (Off mic.)

ADM. HOWARD: Who said that? Come on up. (Laughter.)

Q: I hope you don't ask more questions about the movie. (Laughter.)

ADM. HOWARD: No, I just want to say thank you for participating.

Q: No problem. Thanks for coming.

ADM. HOWARD: No, absolutely.

So someone drops a wrench, and the game's on. All hell breaks loose. Submarines start moving around. And it's always, like, not the sonar tech; it's always that nice, likeable sailor that – you know, the cook or somebody who drops the wrench.

Q: It's the strategic corporal.

ADM. HOWARD: It's the strategic corporal who drops the wrench and creates this fight. That is a great answer. Thank you.

Q: Thank you.

ADM. HOWARD: But when you think about a sailor and a gaming console or a personal device, when they plug it into my government network, they are doing the equivalent of dropping the wrench, right? Right. When you open up the public network like that, you're either beaconing or you're creating a hole. Ooh, and the game is on, trust me. Trust me.

But we have, with this generation – because they grew up in trust, they grew up after the bomb shelter period – I have to teach them about operational security. I have to get them to believe that there's somebody out there looking at them all the time. Except it's more than one person, so it's not as simple as it was in the Cold War. But that everything they do in this, whether it's in their private network, computer, laptop, tablet, or whether it's on my government computer, they're in it.

And here's where it gets really complicated. It's not just my sailors. It's not just the active and reserve. It's every civilian who works for me. That, if somebody wanted to arguably get at me, they don't have to get at my computer. They could go through the administrative assistant, who happens to be a civilian, and get at through her computer.

And then collectively, when you think about databases, we're all at the mercy of different organizations. So whether it's a private company that's been exploited or a government one, we're all – we all have vulnerabilities in this domain.

And I would argue that this idea that you can put your head in the sand and that's an effective technique, it might make you feel good – (laughs) – but it really doesn't work well. And so we have got to figure out how to fight in this domain; and if we're just going to be defensive, how to be the best defenders that there are; and how to give our people the tactics, techniques and procedures to be stronger warriors in this domain.

We also need regulation in this domain. It is the Wild West out there. It is Tombstone, and I don't think we have a Wyatt Earp right now. We know things are happening because we either are – have the effects in our lives or we read about the effects on other people's lives. Or they tell us.

You know, Estonia is a great case, where after their networks were attacked by the Russians they went to NATO and said, this could happen to any of you. And that's, I think, what really propelled them to set up their Center of Excellence in Tallinn.

Next slide.

And literally sometimes that's what it takes. Cold War came back to the forefront for us in the '60s with the Cuban Missile Crisis and the thought that there might be nuclear weapons right there in Cuba. Changed, again, the way we think and how we manage all of this. And so a crisis can propel you to take action.

And what is going to be the crisis for us in this domain? Is it going to be something on the scale of 9/11? Or was the guardian – the Guardians of Peace into Sony, was that sufficient for us to get galvanized to change how we look at this domain and really understand it?

Last slide.

I can tell you, for DOD, we're moving forward. We put out the DOD – secretary of Defense issued his DOD strategy, which we're homeland defense when we're in the United States. So it is about defending our networks. It's about making them resilient. It's about training our people.

But also, for the first time, our Law of War Manual – the new one that just came out – now has a chapter on cyber operations. And it's really very helpful for us because it defines what neutrality is, it better defines what an attack is. It makes it pretty clear from the Law of War – from applying the Law of War principles that we are probably looking for major physical effects in this domain if we're going to consider it an attack. So just defacing a government website would not be considered an attack. But we have got to get through policy conversations and legal conversations in order to provide some framework because we're not at the point where I've got the equivalent of a SALT talk or an INC SEA between me and the other countries in this domain. And without those, we potentially could have a confrontation in this domain, or we'll continue to see it play out with our conventional forces and we might get some misunderstanding at that level.

We're moving along. And it is this great generation of sailors, in my case, who will help us get to an understanding of this domain, how to – how to fight in it and how to protect it, but also how to leverage it in the innovation of ideas.

Last slide.

So that's my app. And with that, I will take your questions. (Laughter, applause.)

MS. HICKS: So we have time for – at least for some questions. I'm going to ask one and then turn it over to the audience.

ADM. HOWARD: Sure.

MS. HICKS: So the one piece of the Cold War app, maybe, that it would be helpful for you to talk about is the deterrence piece of it. To what extent do you think

there is commonality to the way we thought about deterrence in the Cold War and how we need to think about it today vis-à-vis cyber?

ADM. HOWARD: So we're missing one major piece for the deterrence piece. So Frederick the Great once said deterrence without credible power is like music without an orchestra. What is our credible power that we're talking about? And it has to be very visible. People have to believe you have this very – combat power or strength. And we have probably not defined or demonstrated what this credible power is. And so if we're going to get to deterrence, there's got to be the hammer for what we threaten.

And so, in the real world, the nuclear weapons were clearly demonstrated and are a very credible power. So the threat is the counterstrike, and people believe that that is possible. No one has defined for me yet what is this credible power that we're talking about in order to get to a deterrent policy.

MS. HICKS: Yep, good.

OK, we're going to have a microphone that comes around, so when I call you please state your name and affiliation and brief question, please. So we can start right up here in the front.

Q: Thank you very much. I have a quick question.

How many –

MS. HICKS: Name and affiliation.

Q: OK. Todd Wiggins. I'm a freelance videographer here in Washington. I have a quick question.

Have you noticed a growth in potential for female officers in your tenure? And how is – what's the perspective for the future for other females to become admirals or in other positions of power throughout the military?

ADM. HOWARD: Oh. Well, for us – I think for all of the services – the journey starts after World War II because the women were capped at 2 percent of the armed forces and women could not hold the rank of general or admiral. That was changed in '67, and the Navy had its first woman admiral in 1972. And then particularly, I think, for the Navy and the Air Force, it was the repeal of the combat exclusion law that allowed women to go into combatant ships. So in my case, I was able to move into amphibious ships and fly combatant aircraft.

So we've gone from, when I started, about 5 percent women to 17 percent women in the Navy today. We're still an all-volunteer force as well as an all-recruited force, so some of it's still what is the propensity of women to enlist or come in as officers. But in terms of opportunity, we're already had our – for the Navy – for us, really, one of the last

bastions, I think, was submarines, but we've already had a woman as commander of a carrier strike group, more women COs of destroyers and cruisers than I can count.

But what I also remind people, it doesn't matter whether you're a man or a woman. The journey to make one-star is a 25- to 30-year journey. So whatever percentage of women we had when the combat exclusion law was repealed, you're probably not going to see a greater representation of women at the admiral or general level. And so, as the demographics change, then it's a quarter of a century later that it sort of plays out.

So right now, for the Navy, we're about 10 percent. Woman admirals are about 10 percent of the – all of the total admirals, including a few years ago that first woman head of the Seabees, promoted to two-star.

MS. HICKS: OK, right here.

Q: I'm Jeff Broach (ph) with Johnson Controls –

MS. HICKS: It's coming.

Q: – and we are your – (comes on mic) – industry partner for cybersecurity in the Naval District of Washington.

The new battlefront in the cyberwar is control of networks. Attacks there can involve more than data property theft. They can cause significant physical damage by disrupting and sabotaging the controls processes that operate critical infrastructure, equipment and systems. My question is, what is the Navy's plan and budget for protecting these crucial industrial-control systems that are so prevalent in the shore community? Thank you.

ADM. HOWARD: So, for us, in 2013 we had a simultaneous massive intrusion into our networks. And if there was a crisis for the Navy akin to the Cuban crisis, it was that. And so that caused us to step back and look literally tooth-to-tail, inception to, you know, decommissioning, and create an enterprise approach to how we look at the cyber domain and how we manage our networks, what they mean to us in terms of command and control, all the way down to SCADA/ICS in the shore infrastructure. So we have gone on this journey that involves fleet and type commanders, CNIC – our shore commander – and have gone through and have started to systematically map out our architectures and all the variations of software that have been created since DOS. And we're going through that process of mapping that out, and then really getting an understanding of our as-is state.

And then, as we work our way through that, for some of these software systems, we will have to go back and literally sort of create an operations and sustainment thought process; that, as this domain unfolded and software became more ubiquitous and you go from analog to digital, the thought that you might need a sustainment line for software

was not part of our acquisition sort of way of looking at the world. And yet, now we know that you can have zero-day vulnerabilities in your software. And so you really have to have expertise along those lines of code for the life of the software, so that even as the software speaks to other software – whether it's Adobe or resides on Microsoft – as they discover zero-day exploits or other vulnerabilities, you have to understand how that's going to impact your software.

So we are pretty far down that path, arguably farther than a lot of other organizations. But we know it's just going to take time because we are – we're a very large organization.

And NMCI – I once talked to an expert. He said, the only thing bigger than the Navy and Marine Corps Internet is the Internet itself. So we have an issue of scope that we have to wrap our arms around.

MS. HICKS: Good.

OK, anything right up the middle here? Let's take one all the way in the back.

Q: Admiral, Tom Goldberg with Lineage. Thank you for your service. Very much appreciated.

Just to follow up on the gentleman from Johnson Controls, is the Navy intending to use its buying power to move to new manufacturers, domestic-based, move away from what Richard Danzig said is a diet of poisoned fruit?

ADM. HOWARD: So one of the things we have done is we have looked at this – our process of subsea. And when you look at what you need to make sure what are the critical components that you just can't have any sort of defects in – so that, in the end, if that component is extremely critical and it failed, then, you know, the submarine would not be able to get back up to the surface – we have created a CYBERSAFE process. And then now we're going to start wedding that through all the way down to the fleet level, which means we will have to go through our systems and figure out what are the critical CYBERSAFE components and what are the critical CYBERSAFE software and then, after we identify those, figure out what it is that we need to have created in a trusted and much more – you know, large – more significant oversight in terms of the pedigree of that particular component. And that might be a chip. It might be a circuit board. But we're obviously going to have to get to a place where, for certain components, we're going to have to be able to go from inception to installation and know who had it, who touched it, and who built it.

MS. HICKS: OK, last question. I've ignored this side of the row, so the woman right here in the gray. Yes, please. Yeah.

Q: Hi, Ma'am. Lieutenant Liz Clark (sp). I work for Navy Office of Legislative Affairs, for cyberspace and C4.

One of the questions we get a lot – and I'm curious what your take on it – is how do we recruit, train, and then retain our cyber warriors that we're creating, especially after we give them a lot of commercial training which makes them very appealing on the outside?

ADM. HOWARD: So the one – I don't – right now we don't have an issue recruiting or really retaining our people. And I will tell you my experience has been, whether it's a nuclear-powered engineer or an aviator, people stay in the service for the reason they joined – that sense of purpose and patriotism. There will be exciting challenges and opportunities, particularly warfighting opportunities, in this domain that cyber warriors arguably will not get in the civilian world. And so the same sort of adventure and excitement that makes a SEAL stay in will probably be the same sort of adventure and excitement and of mission accomplishment that will cause a cyber warrior to stay in.

But I also want to remind you of something, that when somebody asks me how many cyber warriors we have, I go we have 326,000 active, 59,000 reserve, and 200,000 civilian cyber warriors – that we are all in this domain, and that we all could be exploited, we all can create a vulnerability. A civilian can put their thumb drive in a – in a government system just as easily as a sailor can. And so we're all in it and we're all warfighters.

Thanks.

MS. HICKS: Well, I want to thank everyone for coming this morning. I want to thank Rolls-Royce North America, that sponsors this Military Strategy Forum Series. And most of all, I'd like to thank Admiral Howard for her great presentation and leadership at the Navy, and we look forward to seeing more of you going forward.

ADM. HOWARD: All right.

MS. HICKS: All right. Thanks.

ADM. HOWARD: Kathleen, thank you for your time this morning. (Applause.)

(END)