Center for Strategic and International Studies

The Role of the U.S. Military in Cyberspace

Keynote Address:
Lieutenant General James K. "Kevin" McLaughlin,
Deputy Commander,
U.S. Cyber Command

Panelists:
Aaron Hughes,
Deputy Assistant Secretary of Defense for Cyber Policy,
U.S. Department of Defense

Major General Paul M. Nakasone,
Commander, Cyber National Mission Force,
U.S. Cyber Command

Dr. Paul Stockton,
Managing Director, Sonecon LLC;
Senior Adviser (Non-Resident), CSIS

Harvey Rishikof,
Senior Counsel,
Crowell & Moring, LLP

Introduction:
John Hamre,
President and CEO, CSIS;
Pritzker Chair, and Director, Brzezinski Institute on Geostrategy

Moderator:
Dr. James A. Lewis,
Director and Senior Fellow, Strategic Technologies Program,
CSIS

Location: CSIS, Washington, D.C.

Date: Friday, October 9, 2015

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

JOHN HAMRE: Good morning, everybody. Thank you for coming. It's such a lovely day. You know, if we were really smart we'd be outside, but instead we're going to be educated and we'll stay inside. It's easier to do that, and I want to say thanks to all of you for coming.

Before we do public events we always have a little safety announcement. I'm your responsible safety officer for today. Nothing's going to happen, I want you to know that. But if something does happen, I'm going to ask you follow my directions. The exits are right back here. The stairwell that goes down to street level is right off from that exit. If our problem's out in front, we're going to go that way. We'll meet across the street at the National Geographic in their plaza. If the problem's out that way, we're going to move across the street to the park. Just follow me if we have to, but I'm confident we won't have any issues. Thank you very much.

This is a – this is a pretty big subject today. And I had the privilege of talking with General McLaughlin. I got to brag here. I mean, he was a military fellow at CSIS now 13 years ago. And I'd have to say, it's been – I've needed an X-band radar to keep track of his trajectory after he left us. He's just done a fabulous job and, of course, now is the deputy commander for CYBERCOM. Lots going on. We're thinking through a lot of big issues right now, organizationally, with the Cyber Command.

And we're at that stage, what is the way that our government is going to structure itself to be more effective? There's a big debate, he cannot talk about it so don't ask him the question, what's going to happen with the UCP? But there will be a UCP. And we're going to start seeing, moving our way towards, I think, a more predictable and efficient structure as we understand that this is now the primary theater of combat going forward. And we're going to have a chance to explore those issues with him.

So I want to say thank you to him. I'd also like to say thank you to Paul Nakasone who's here, who's going to be joining us on the panel. Paul Stockton – thank you, Paul. Harvey Rishikof, you know, these are great friends. I'm very pleased – I don't know Aaron Hughes, forgive me for that, and so I'm going to have a chance to meet him. But to have their join this and help us illuminate the issues – it's going to be a rich morning. But the best is coming right now. So would you, with your applause, please welcome and thank Kevin McLaughlin. And we look forward to hearing his views.

LIEUTENANT GENERAL JAMES "KEVIN" MCLAUGHLIN: Dr. Hamre, thanks for the great and kind welcome. It is a treat to be back at CSIS. I've been back since I left as a fellow, but I have highest regards for this institution that plays such an important role in very complex matters. The topic we're going to talk about today is an area where I know you continue to lead. Senator Warner, it's great seeing you today as well. Thank you for all your service and your leadership in these areas as well. I know you have more to give too, so we're looking forward to that.

Before I get into my remarks, you know, information sharing's been a big deal in this area. And CSIS is great in the information sharing. And today, you're broadcasting this out over the Internet. And sitting in Chandler, Arizona is my mom watching. So, hi Mom. And but what

I would ask, if any of the critiques that are on the negative side, please don't put them on the Internet. She'll be watching, and you'll probably hear from her soon.

Well, today what I'd like to do is really to hopefully tee-up some of the thorny issues and the hard work that's going on on the DOD side of things in cyberspace, and really maybe tee-up the panel that's going to come subsequent to my remarks. I'm going to accomplish two things at the same time. First, I'm going to give you a broad overview of the five goals that were just recently articulated in Secretary Carter's – when he signed the new Department of Defense cyberspace strategy.

And so, as I kind of go through those, in each one I'm going to go into the details of U.S. Cyber Command's – our mission, what we're focused on, and sort of in the context of that broader – that broader strategy. And at the end, you know, what I want you to do is you know what our mission is, what's different between what DOD, the Department of Defense is doing in cyberspace than other parts of the government, and to understand where we are in the generation of the capacity and capability that we need in this area of operations. And so if that makes sense to you, that's the way I'm going to proceed.

So that's a new strategy that just came out. The first thing that it really – it acknowledges that within the Department of Defense cyberspace is a domain of operations. And so for us, there are a lot of common areas in terms of how we think about operations and all the other domains with cyberspace. We're trying not to reinvent the wheel in those areas that we don't need to. But there are a lot of unique parts – unique aspects of this domain and how we operate in it. And we certainly have to account for that.

So with that as the backdrop of how we think about cyberspace in general, let's talk about the first goal that's in this new cyberspace strategy. And that is focused on building within the Department of Defense capability and capacity to operate in cyberspace. So there's a significant amount of investment occurring right now in the department, and a lot of activity not only within Cyber Command but within the service components that support our command. And I want to just explain what a few of those are to you. You may have heard about some of them, others perhaps not.

The first is starting in fiscal year '13, even with budgets tight, resources tight, the department embarked on a journey to create between fiscal year '13 and the end of 2016 133 separate cyber teams. And we are generating over 600,200 additional operators from all the services to man what we call the cyber mission force. So these cyber teams are being provided by all the military departments. So each of the services have roughly built about a third of those teams. We're over halfway through the creation of those teams. By the end of 2016, all the teams will be in place and at initial operating capability. And by around the end of 2018, we expect all those teams to be at full operational capability.

So this is a – this is probably the major element of what we would consider our tactical force that did not exist before 2013. So you can imagine the work that's occurring right now to basically generate the ability to bring onboard all of these men and women that comprise these teams, to get them trained, get them into teams that never existed, and to begin to use and operate

those teams. And what's happening right as we create them, we're already using them. So these teams – and as I talk about our mission I'll be able to describe what these forces are already doing, even though we're just barely halfway through the build of the cyber mission force.

The other thing that's occurring and we're spending a lot of resource on is we are generating the ability to then train and exercise and ensure the readiness of these teams. So if you think about all the ranges that exist, you know, we have Fort Irwin where we train advanced training for the Army. We've got the Nellis Test and Training Range where they do it in the Air Force. We're doing the same thing in cyber. We're creating the environments, the range environments, the capacity to build – have opposing forces or aggressor forces, to build scenarios and to let our people, both individuals and sub-elements of these teams and then multiple teams, plug into an environment and train in a realistic manner.

And to do it – what we're resourcing now is the ability to do that seven by 24 – you know, seven days a week, 24 hours a day, we want people to be able to log into this environment anyplace where they live in the world and do realistic training. The – as you can imagine, the ability to have – the need to have the sophisticated technical skills along with what's growing is the operational art about how this works have to be tested and trained and our people have to prove and demonstrate that they can do their job in a realistic scenario.

If I mentioned that this force is the tactical force, well, in all military operations and domains you also have to have the ability to take guidance from higher headquarters and, you know, combatant commanders and translate that into plans and then operations and command and control forces. We're creating that layer as well within the Department of Defense. So between U.S. Cyber Command, between our components, and the combatant commands, we're generating both the ability to conduct planning and to oversee operations and to command and control very complex operations – not just cyber alone, but cyber operations that are integrated in with the other domains of operations.

That is something that's evolving just as rapidly as the creation of these forces. It's not simple. It's not – it's sometime controversial. There's debate about how it ought to be done. But we are moving from the debate intellectually to, now that we have forces, you know, what we're doing is the way the military always operates. We're letting practice – you know, actual experience and operations inform how the doctrine ought to be – ought to be shaped. And we're really in that stage now. And that's an exciting area that's evolving rapidly.

Now, the last thing I want to mention to you here, just so – because I do want to make sure we have plenty of time for questions – and that's culture. Part of building capability and capacity in this area is thinking about the culture that is required to have cyberspace as an operational domain. You know, there are two kind of key areas there. The first I thinking about this as an operational domain drives a different culture than if you think about it just as a communications and information technology domain, or just an intelligence operations domain. It's not really a functional area for us. It's an operational domain.

So thinking about how military forces operate and plan and what type of – what type of doctrine's required, that is a different approach to operations in this domain than the way we

perhaps have thought about in the past. But also, almost every negative thing that happens in this area – and it's not just in cyber – where an intrusion occurs, you know, something bad happens from a security perspective, for the most part the vast majority of those are always because there was some failure at the human level.

Somebody clicked on a spearfishing email, they had a practice that was not an accepted practice. They didn't have the cyber terrain upgraded or patched appropriately – all things that we know to do. Typically the problems that we have is because that wasn't followed through on. And often the leaders of those organizations didn't make it a priority. You know, most organizations in the military aren't cyber organizations. You know, they conduct – they do other missions, but they all now are part of the cyber domain. So accountability to the individual level and really at the leader level is a key part of the cultural change that's occurring.

And we're beginning to see, you know, if there's an inspection or if there's something that happens where there's a weakness out someplace in the field, that's getting visibility very rapidly and senior leaders are held accountable for this mission as well. It's quite different than what we would have seen in the past, where perhaps it would have been the J6 or the communicator in the organization that would have been held accountable. We're not holding leaders accountable. And I think that principle's important, you know, really everywhere, not just in the military. So that's our first DOD goal is building capacity and capability. And it is a major focus for us and it's something that we're being held accountable for at a pretty high degree of fidelity.

The other – the next three parts of the goals really align with our missions. I'll just go through them quickly, but that first mission of U.S. Cyber Command and the top priority according – from Secretary Carter is the second goal within the DOD strategy, and that is to defend the DOD information network and to secure the data within that network. So job one for our forces as we build these teams, as we – as we organize ourselves, is the defense of the DOD information network.

And that's not just the – you know, the IT network that connects our computers where we send email back and forth and, you know, where we log onto applications. It's all of the ways that we connect platforms, our command and control systems, you know, everything that either uses computers to communicate or has computers or embedded controllers in it is part of the domain that we're responsible for defending.

So it is our top priority. We are increasingly attacked in this area, so the threat is significant across a range of types of threats. And it is something that – you know, I get asked quite a bit what keeps me up at night? It's this mission area that is most important, and it is the one that probably keeps us up most at night, and that is: Are we ready, and will we be ready, to take these new forces and ensure that we are able to defend this critical part of the Department of Defense's mission?

The second mission of the command, but also – it's also linked up with one of the goals of the strategy, is to make sure that we do full-spectrum planning and build viable options in the cyber – in the cyber domain that we could use in support of combatant commanders around the

world. So these forces and these cyber mission force teams and these intermediate headquarters, they are all linked to a combatant command, because those are the commanders that we charge with operating inside the military. And we're bringing the cyber capability that each of them need.

And so the key for us to make sure that our capabilities, as they grow, are integrated in with their plans, that they're integrated in with their operations, with their exercises and training, so that – so that each of those combatant commanders has the ability to operate in air, space, land, sea, and cyber. It's just that our command is charged with bringing those teams and that capability forward. And that is our second – that's the second area of our mission focus today.

The fourth goal within the cyber strategy and our third mission is, to me – is probably the one that's the least developed at this – at this point, but it's also very important. And you will still see things in the open about it. And that is to defend the United States against cyberattacks of significant consequence. Now, I do want to be clear, in a lot of audiences, the responsibility of DOD in this area versus the Department of Homeland Security or the Federal Bureau of Investigation or other parts of government is sometimes not clear. So again, our main job is defending the DOD information network and providing capabilities to combatant commanders.

But in this third mission if there was an attack of significant consequence we are building the quick reaction forces and the capacity to defend the broader United States against an attack. It could be an attack against critical infrastructure. It could be something that rises to a certain threshold where we will be asked to come in and assist. In every case that we currently imagine, we would do that in support of another government agency. So we don't expect we would have Cyber Command forces out maneuvering, you know, on their own, you know, in other critical infrastructure within the U.S. – non-DOD infrastructure.

But we absolutely could envision being asked to bring capacity to support the Department of Homeland Security or the Federal Bureau of Investigation, depending on the nature of the threat, and to operate that way. So we haven't done that to date. We've been involved in some areas where we have potentially been planning that, if asked. And we certainly are exercising – doing a lot of tabletop exercises and war games thinking through how we would do this, because you can imagine it's a complex policy and legal framework that we would need to operate on to do this.

So those, very quickly, are the three missions. I've gone through four of the goals. And I'd like to talk about the last –the last goal in our strategy. But it really forms the basis of a very exciting framework for us to think about our daily job. And that is the direction for us to have innovative, forward-thinking collaborative partnerships in the cyberspace area. And they really exist in sort of rings for us. Certainly we have to operate in a way that's beyond what we typically have been comfortable doing with other parts of the military – so, other combatant commands.

Cyber warfare doesn't just live nicely within one – with one either geographic area or one functional area. So the partnerships we have with the broader combatant commands and other parts of the department are – have to be different than what we have in other areas, the same

partnerships we need with other parts of the federal government. So we have real-time integration with the Department of Homeland Security, with FBI.

They have LNOs in our spaces. We have people forward deployed in theirs. And we operate with them. Not that we have each other's authorities, but we share information, we plan together, and we conduct synchronized operations with those parts of the U.S. government. It's absolutely critical that we can do that in cyberspace. And while it's – we have more to do, I'm excited about the aggressiveness across all these other partners to want to move forward together.

We have to have the same type of collaboration and partnerships – and this is an area where I think we have a lot of work to do – with industry. You know, how do we share talent? How do we onboard the latest technology that we can take advantage of quickly, before that technology – you know, in cyberspace it doesn't take long before that technology's no longer really the latest. And so we can't take a year – you know, years to bring it on board. We have to bring it on board rapidly. So how we partner with industry in a couple of dimensions is part of this direction.

How we do it with other countries and with our allies? And so I've had a lot of experience earlier in my life in the space side of things in the military. And I've watched cooperation sometimes take years and years to sort of build a framework for how we might partner together. We're trying to drive that cycle time down to, you know, months of how we do things with a variety of countries so that we – because we have a lot of shared concerns, we have shared interests. And just like we do in other domains, we would like to be able to operate as partners in cyberspace.

And so the collaboration in this area across all those sectors is critical. And it is – it's a focus of the department. So as I get ready to conclude the remarks, because I really want to take your questions, if you think about those five broad goals, there have been a lot of strategies written where the goals is – you know, you finish the task when you write the strategy. You know, you write it, you put it on the shelf, you put a glossy pamphlet out, and you say that I'm done.

In this case, we have a – our team is focused on implementing the strategy with aggression. And it's not just U.S. Cyber Command's responsibility. We have – we have partners across the DOD that are charged with implementing this strategy. But it is something that right now we are working to get implemented as quickly as we can. And there's a lot of leadership attention on following through on it.

And the reason that I talked about our mission in the context of it is it's a very focused strategy, it's a realistic strategy that's driving what we're actually doing, as opposed to something that's in theory. And I think it's pretty exciting to watch it take shape right, you know, in front of us at the same time that our cyber forces and the way we think about operating in cyberspace is taking shape as well.

So I'm really pleased to be here. This is an important topic. Just the nature of the audience, I think, gets at many of the points I've made about collaboration and basically being transparent about what's going on in the department. And I think the question and answer session, I think, hopefully will extend that. And I know that the panel that we'll have afterwards with even put a fine point on that. So thank you very much. (Applause.)

JAMES A. LEWIS: I'm supposed to run interference. I don't think I really have to. But that was a great presentation. And why don't we – I have a lot of questions, but let's give you the first crack and see what you thought. Do we have – oh goodness. How about that person there. Go ahead. If you could stand up and identify yourself. We have microphones that are coming.

Q: It doesn't work? OK. Thank you. My name's Xu Zhel (ph) from China Central Television.

As we know, the United States and its coalition continue airstrikes against ISIS. But at the same time, we can see the threat of cyberattack from them. For example, the FBI was warning that a group of ISIS hackers is threatening U.S. government website. So how much are you concerned about this? And what kind of measures or role does U.S. Cyber Command play or have against ISIS? Thank you so much.

GEN. MCLAUGHLIN: Sure, thank you.

Well, our concern with ISIS specifically has been in a couple of areas. The one that's been the most visible within the military has been their public release of U.S. military member's names, you know, their pictures, where they – you know, their addresses. You know, they're trying to generate fear, you know, among our – the people that do the job. So that has been – Cyber Command has not much responsibility there. The real issue there – that's a department-wide concern. But that is an example of how ISIS is using cyberspace and the information that they can pull from cyberspace to generate a threat.

Where you move directly into Cyber Command's responsibilities or concerns is if you see any actor – it could be a non-state actor like ISIS – if they mature their ability to where they could actually move beyond, you know, website vandalism, you know, to nuisance type of attacks, but move into where they could actually increase their skill, like we see from other actors, where they could actually threaten the network, you know, do a destructive attack in cyberspace.

Those are all things that we see occurring in this area. So we watch very closely go – of any actor, including ISIS, to see – are they – do they have, A, the desire to move to that level and then would we be ready to counter that, if they did. And so today I would say we're watching it closely. We don't really see them as a threat at that level. But it is something that in this area all it takes is the right intellectual framework. And you can – you can get there very quickly in cyberspace. So it's not something that we discount as a potential concern.

MR. LEWIS: OK. The gentleman there.

Q: Good morning. Michael Lucero (sp) of CGI.

Understanding that doctrine on the defense side and policy on the civilian agent side really drives acquisition, and we have this important goal of being prepared for that significant cyberattack, how would you try to join these two efforts together? What would be a primary focus if you could encourage policymakers to join these doctrine and policy development efforts together to really prepare for that cyberattack?

GEN. MCLAUGHLIN: From my perspective right now, we're seeing that convergence of what the policymakers are driving and what we're actually doing practically both in technology and the fielding of capability. Even the strategy itself, you'll see – most of it's available, you know, to the public – has a very strong convergence of strong policy-related direction and guidance along with the resource and the technology and the capability fielding that we have had within the Department of Defense. So I think there's good convergence there already.

The real question is, at this stage what's the size of the eventual bills? You know, how much investment's required not only to secure existing cyber – you know, it's not just cyber networks. All the weapons systems and the things that we've invested, you know, billions of dollars in, maybe trillions of dollars in, is fielded and has been – and that we've been using that for decades. So making sure that we understand any of the vulnerabilities that exist in the fielded systems, that we prioritize any improvements that are needed, is a key focus of the – so the policy's there to do that, and then the technical solutions and the services will follow with prioritized funding.

But then as you build new things, equally important – anything coming through the acquisition system, you need to make sure that you're paying for the cybersecurity attributes of those and that they're funded and viewed as an important requirement as well. So it may be looked on the outside that those areas either aren't connected, or aren't connected in a significant way, but I think the reality is that they're tightly coupled now, and it's senior leadership in both policy and sort of material acquisition communities are engaged in a constant senior-level dialogue on how we move forward.

MR. LEWIS: How about the person in the white shirt there. We're going to have a lot of questions, apparently. I hope you're ready.

Q: Hi. Sean Lyngaas with FCW.

What's your process for prioritizing defense of critical infrastructure? You know, you mentioned it's part of your charge to defend the homeland from attacks on critical infrastructure. You know, Sony Pictures was deemed critical infrastructure because it's a movie sector and that's one of the 16 sectors that DHS deems critical infrastructure. So would you be called on defend something like that in the future?

GEN. MCLAUGHLIN: Well, so, let me answer your question, and maybe first let me answer from the department's perspective. We do have – we're developing our own process within the Department of Defense to prioritize critical cyber infrastructure or critical cyber terrain. So we both have the part of the department that looks at critical infrastructure broadly. And so we're making sure the cyber elements of that are woven into those – into our vision of DOD critical infrastructure.

But we're also learning, if you are charged to defend a specific mission area, for example, or platform – take, like, a missile defense network – we have invented, at least for our way, to go into a complex network like that and prioritize the critical terrain within a distributive, complex network to understand what has to exist and be functioning in the face of an attack. How do you make that part resilient? How do you actively defend it so that a commander can still get his or her job done when that mission has been threatened, or is under attack? So your question, on the DOD side, is important for us. And I think we're building the framework for how we think we ought to do that.

Within the broader U.S. critical infrastructure, you know, there's – the prioritization there, you know, happens ahead of cyber. DHS really – the Department of Homeland Security I think is the primary part of the U.S. government that's touching each of those critical infrastructure segments. They talk to them routinely. They generate exercises and train. And so they're the main locus of activity there. Our job really is trying to understand what are the – if we're going to have responsive forces there that are going to have to respond, how do we make sure that the people that are on those teams are trained and ready.

For example, industrial control systems. It's quite likely that terrain could involve those networks that monitor power, electricity, and transportation. And so that type of terrain is a little bit different than normal networks. So we're building teams that understand the industrial control systems, the embedded controllers there, and how they operate and how you –

(Section break.)

Q: (In progress) – makes the decisions and acquisition. And we still see here a lot of acquisition of fully-made equipment and technologies out there. We're still putting in high-bid highways. They were not meant to be like that. So is there a plan for that – immediate plan that when you do procurement acquisition and you train the folks who are basically making the acquisition decision, which in some case they don't understand that piece. And we have to end up educating them in there. So what's your – I think that would be a recommendation for me to make, a fast track, you know, moving that and just engage them in integrating the cultures out there on both ends. Is there a plan for that yet?

GEN. MCLAUGHLIN: Sure.

So that is a – so that has been a weakness. And it is a – it's an organizational culture of weakness. It's not necessarily an individual culture of weakness. The way that we're dealing with that, and I mentioned to you as I mentioned in an earlier question, is we think about fielding new systems. In the past, I would say the cyber elements of an acquisition were really viewed as

ways to make things more efficient and more effective, save money. You know, it was – it was using the technology in those areas without thinking through what vulnerability, you know, that might be created by using cyber technology and some new – you used an example, but in some new acquisition.

All we're really doing is making sure that in the process of determining what you actually field, that the cyber vulnerability is – in the design and the concept of operations is highlighted and raised forward in the broader decision of what you're going to – how you're going to build it and how much you're going to invest in the cybersecurity elements. And the Department of Defense is going to make sure that those criteria are met before they allow new things to go forward. That's the real change in the organizational culture, is having that discussion early and having a decision maker high enough up that cyber security is part of their concern and that it's one of the requirements that's going to be – that's going to be met whenever you field some new capability.

MR. LEWIS: OK. How about the – could we get both of your questions at the same time? That'll make it a little easier on the – hold on. And could you identify yourself, please?

Q: I'll shoot, and then I'll hand it to him. So, Patrick Tucker, technology editor with Defense One. Either of you could take this.

A lot has been made of the need to deconflict the airspace over Syria as a result of Russia having launched an air, ground and sea campaign. Is there any concern or evidence that the presence of Spetsnaz units in Syria could compromise U.S. cyber operations in that country? And have you observed any change to the information environment as a result of their presence there?

GEN. MCLAUGHLIN: Yeah, so I wouldn't comment on any ongoing operations in that area. I would tell you that any place the U.S. military is operating, our concern is not only our own cyber terrain and how we're operating and defending it any theater – it would include operations in Iraq and Syria – and if there are any players that are potential threats or bringing capability that would cause us concern there, we will track them – we'll track them to a high level of, you know, detail, to make sure that we understand what threat them might pose to our networks or our forces, and that we're ready to defend against it or deal with it. And so I wouldn't want to comment in specific on any particular actor, but that is what we do everyplace we're operating in the military.

MR. LEWIS: And then Joe.

Q: Joe Marks from Politico.

Wondering first if you have a timeline for that 24/7 remotely available training environment that you talked about? And then second, the DOD cyber strategy envisions more – or gives more ink to the possibility of offensive actions than previous versions did. Can you talk a little bit about how you're training for offensive in that environment?

GEN. MCLAUGHLIN: Sure.

And so, first, on the broader – the broader timeline of when we think we'll have this capacity to train constantly, we have an initiative we call the persistent training environment. It's really a combination of the range, the virtual place where forces will train, sufficient capacity for our aggressor teams, you know, our opposing force, the ability to basically write scenarios and scripts and to, you know, plan very specific training, and then to assess the performance of teams that are training and provide that feedback, back to both individuals and teams. That's the broader concept of a persistent training environment.

It is an initiative right now that we're – that's in deep discussion in the department about – you know, when we're looking at the FY '17 budget, you know, that we would like to put in. So it's still too early to determine how much funding we'll get. And that level of funding – we think there's strong agreement that this is an important capability that will be there. The amount of funding we get sort of in the – our DOD budget will drive when it will be ready. But we are – we already have parts of it in place. So you know, we've been funding it. And so what we have today is the ability to do that type of training. We just can't do it with as many teams and with – as often as we need. So what we're really trying to do is robust it out. So we're still a few years away. And if we get the amount of money that we were asking for before, we'll have the seven by 24 capability.

In terms of – in terms of making sure we have the ability to train both defensive and offensive teams, we already have the ability to do that. So we – again, it's really the lack of capacity to do it as often or as much. But we have a very similar approach. We take teams that would have an offensive mission. We put them in a realistic environment with an opposing force, someone that's simulating the adversary. And they have – and they go through a series of scenarios so that those operators are able to show that they could do their job in a realistic environment. And so we have that ability today. And we have the ability to certify entire teams in their mission today. And the goal is we want to certify – you know, we want to give them more repetitions to do their job. So but we think about that training just like we do really in any other domain. It exists today. It's just not – it's not as often or the capacity that we need.

MR. LEWIS: How about the individual there at the far end? Red shirt. Should have picked someone closer to the microphone.

Q: Thanks so much. Zach Biggs with Jane's.

You mentioned a little bit about the threshold at which the mission force would be assisting DHS, for instance, in protecting. Obviously that threshold's a hotly debated topic. It's also been debated whether it should be a little more public as a deterrence mechanism. I want to ask you, do you feel like you fully know what that threshold is, and by extension senior leadership within the military? Can you tell us anything about what the thought process is as to how that threshold works? And how does something like OPM – which might be considered espionage in some areas because it was a breach and not really destructive – how does that play into the notion of a threshold?

GEN. MCLAUGHLIN: Sure. A great question.

So I do think we have the broad framework for what the threshold looks like. So if you consider, you know, the current definitions, really, if you see attacks of significant consequence, so attacks that might involve loss of life or, you know, again, significant consequence to, you know, causing serious damage the United States either economically or in some other area. So we have the broad framework in place. But you mentioned OPM or something else. There are other – there are instances that could occur that are, you know, sort of still – it's ambiguous until it's looked at carefully by the leadership as to what – has this triggered the need for DOD to bring capacity?

One way that we're really, I think, trying to get – drive more clarification into the practical ways, as it were, is by planning and executing some exercises. We have one that I think is the premier area in this for us. We call it Cyber Guard. And that is an exercise that we do annually. We'll do the next one next summer. The most recent Cyber Guard was an example. It was a series of scenarios that were not DOD cyber scenarios. They were off-DOD scenarios. You know, you could think about a cyber threat against a port or some other key critical infrastructures we were talking about.

And we had Department of Homeland Security that really played the main lead in – even though it was a Cyber Command-sponsored event, DHS really built the framework for what the scenario ought to look at, specifically to not only train our people but really to tease out what are those legal and policy touchpoints between industry, between other parts of the government, and between cyber forces, between the national guard forces. We had some – we had some observers from some other countries.

What are the touchpoints so that those senior policy makers could go back – that they go back and continue to refine what that framework looks like that you're describing, that informed, you know, a real scenario? It informed them of what the issues are and what types of solutions might be required either legally or from a policy perspective. So each one of those Cyber Guards has taught us more about it.

So I think we're now in a – I think we feel comfortable that if one of those events happened today you'd see the right discussion about sort of the political leadership, you know, has this reached that threshold? To be honest, it will never be black and white, have a perfect recipe. There's no real event that's that way. But we have a structure within the government to have that discussion, and the ability for a request to come forward where U.S. Cyber Command forces would go – would be put into action. So we know how it would work. We're still refining it. But we could do it if it was required today.

MR. LEWIS: Thank you. One more? How about Ellen? How can we say no?

Q: Hello, General. It's Ellen Nakashima with The Washington Post. It's good to see you again, twice in one week.

GEN. MCLAUGHLIN: Good to see you again.

Q: I have two questions. The first is, now that you're building up forces and capabilities, to what extent can Cyber Command gather information – intelligence on its own, insight into other adversaries' networks, independent of NSA, right? To either – whether you're doing OPB – or, OPE or just to figure out what your adversaries' capabilities are? And number two, it's been about two weeks since the agreement between President Xi and President Obama. Have you begun to see any change in behavior by the Chinese in terms of a tailing off of activity and economic espionage into our own U.S. companies?

GEN. MCLAUGHLIN: Sure.

So to answer your first question – actually, let me take your second question first. So the – I think any changes you're going to see, you know, as a result of the agreement between – that was announced between President Obama and President Xi, I think you'll see that, you know, any changes they'll play out over a longer period of time than just the last, you know, couple weeks. And so I think that's – the answer to specifically to are we seeing any changes there, I think it's too early for any of us to see any of those changes.

On your first question, the nature of operating in cyberspace, really whether – to be honest, whether it's not defensive teams, your offensive teams, they have to have the ability to operate and have access within their networks to whatever their mission is, whether it's learning about the adversary from our blue networks out defensive teams have or if it's – if you're going to deliver effects in cyberspace, you absolutely have to be – you know, know about the terrain that you're there. So a byproduct of what our teams do is they generate insight into those networks.

It may not be – it may not be by the same team of someone that would be operating in the intelligence community, but the information that we have access to is adequate for what we need, and it – you know, in terms of the information itself, may be very similar. But our teams will have a pretty strong ability to generate those insights from doing intelligence, surveillance, reconnaissance within the networks that we need to do our mission, whether it's offensive or defensive. So it's a skillset we expect our teams – our teams do have. They continue to mature.

MR. LEWIS: Well, I apologize to the folks who had questions. We're going to have to do this again, because we didn't exhaust the pool. But the general does have a day job. And we promised we'd get him out of here at 10:40. So we're well-past our departure date. Please join me in thanking General McLaughlin. Thanks for your remarks.

GEN. MCLAUGHLIN: Thank you very much. Thanks. (Applause.)

(Break.)

MR. LEWIS: Am I on? I guess I am. I can take up the remaining hour reading the bios of our panelists, so I won't do that. Instead, I'll just go, not in any particular order.

Major General Paul Nakasone, promoted in June, right? So congratulations.

MAJOR GENERAL PAUL NAKASONE: Thank you.

MR. LEWIS: That's an important step, that second star. Very grateful that he's here.

Deputy Assistant Secretary Aaron Hughes at DOD for Cyber Policy. I think some of you know him. Comes from In-Q-Tel, which is a great background for this kind of stuff.

Paul Stockton, who was the assistant secretary for homeland defense at DOD, and therefore is also another expert on this.

And finally, Harvey Rishikof – last but not least – who is the chair of the American Bar Association's Standing Committee on Law and National Security. And many of you know him for the immense amount of work he's done with DOD and with other places.

With that, why don't I ask the panelists if they could briefly go down the line and talk about what we're here to talk about today, which is DOD's role in homeland defense. And Harvey, we'll start with you.

HARVEY RISHIKOF: Oh, I thought we'd start with the far right. (Laughter.)

MR. LEWIS: Start with Paul? OK.

MR. RISHIKOF: Yeah, start with Paul. Absolutely. OK Paul.

MR. LEWIS: Paul?

MR. STOCKTON: I'd like to drill down into the question of the defend-the-nation mission. What would actually be helpful to the owners and operators of critical infrastructure? And how do those needs for support match up with what Cyber Command might be able to provide?

Let me offer some very preliminary thoughts just to get the discussion going. First of all, it's possible that General Nakasone could devote Cyber Protection Teams to critical infrastructure protection. It's possible. Difficult authorities issues that Harvey will get into, and these are very scarce assets. The Department of Defense number-one mission is going to be defend DOD networks and information capabilities, so there's not going to be a lot of spare Schlitz to go around.

Let me give you a couple of other suggestions on promising avenues for progress. And Cyber Command is already pushing one of these, and that is rely on state National Guard forces to be able to provide support to their electric, water, wastewater, other critical infrastructure utilities. They're right there in the state. They may have some advantages in terms of operating under a governor's authorities. And because they're right there in the state, they can train on the operating technology systems in collaboration with the utilities in a way that's going to be essential for mission effectiveness.

Let me suggest a second avenue for progress that's a little bit out of your lane, Paul, and that is we need to do more to develop business models that enable privately-owned utilities to be able to get revenue so they can strengthen their ability to provide power no matter what to defense installations, even if those utilities are under cyberattack. Many military bases around the nation, they depend on the flow of electric power, water systems from outside the base. We need to find ways of capturing revenue from those bases when they pay their bills to increase the resilience of utilities because those utilities, folks, they could be under attack.

Thank you, Jim.

MR. LEWIS: Thanks, Paul.

Anyone else want to jump on that one? If not, Harvey, go ahead.

MR. RISHIKOF: I would say that when you look at the picture – first of all, than you Jim and John for putting this together. This is exactly what we need, more forums.

But when you think of the scale issue when you are thinking of a cyber problem, you historically have four large hammers that we use in the United States. And the first hammer is the tax code. That's how you influence people to do something. You also have insurance premiums in the private sector. That's how you move America. In my field, we have something that's called lawsuits. That usually focuses people inside the system. And finally, we have regulations or statutes. Now, those are the four major ways we think of the problem if you want to provide a level of security.

So in the DOD context, what we're using are the DFARS. So the DFARS are raising the game for the system for procurement.

And then the issue of insurance, increasingly we're talking about cyber insurance for the private sector, because the irony which is this field is that it is a domain that DOD has classified, but we always say 90 to 95 percent of the domain is owned by the private sector. So it's a unique phenomena in which DOD is experiencing not only the platform, and it's using platforms that are controlled by the private sector. So that's why the threshold question came up in the first panel, because as a legal matter you are always looking at at what point – we used to call this when I was at the FBI the handoff – at what point are civilian capabilities overwhelmed and require DOD to come in because of its volume and size.

And that's sort of the interesting question that has always confronted us. The Center is very involved in that area, of trying to figure out how you do that while maintaining the understanding of what our traditional authorities are.

So Paul has mentioned the authorities. And in this field we have a range of authorities, which is, first, Title 6, which is homeland security; Title 10, which is historically the armed forces; Title 32, which was mentioned, which is the National Guard; Title 40, which is the public buildings and property, works; and finally, Title 50, which is the intelligence community. So we

always talked about, how do you combine all these authorities from a legal perspective to allow DOD to perform its function and the USG?

And we've been looking at this now and thinking this through for a variety of years. But what's really, I think, caused us to respond, to put it at the forefront, has been Sony and OPM have clearly demonstrated to the world that this is a new era that we're involved with, and how do we respond effectively in the system is how I would frame it for you.

MR. LEWIS: Great.

Aaron, did you want to—

AARON HUGHES: Yeah, no, I mean, I just want to make sure that we understand here that cybersecurity is a whole-of-government kind of domain, right? So DOD has a key mission, but in partnership with the Federal Bureau of Investigation, in partnership with Homeland Security. DOD has, you know, the key role in defending against attacks of significant consequence, but that's, again, in partnership with our other government partners. And DOD will bring capacity to bear in a supporting role, but we need to make sure that folks understand that DHS, FBI have that role as well.

I would second what Paul said. As a member of the Air National Guard, I think that the Air National Guard can, and broader National Guard and Reserve force, absolutely have a role in partnering to protect critical infrastructure as well. And my office is working on policies to better articulate how that could happen.

MR. LEWIS: General, want to add anything?

GEN. NAKASONE: Sure. So, first of all, for Dr. Hamre, Mr. Jim Lewis, and great to see you again, Senator Warner, thank you very much for inviting us all today. I think this is a great topic.

We operate in the ones and zeros in this domain, but let me put that aside and talk about the people in this domain. You heard General McLaughlin talk a little bit about the 133 teams. Let me talk to you about this millennial force that we're leading right now in building. So, for the National Mission Force, which I command, roughly about 40 teams.

If you were going to take a look at the team, what would the team look like? Well, the team would look something like this: 80 percent military, 20 percent civilian; average age about 24 years old – so I bust that average just a bit. (Laughter.) The next thing you would see is you would see a(n) incredibly well-trained force. This is a force that has been in training for somewhere between 10 and 27 months, that operates well in terms of on-net operations, that speaks many languages – Java, JavaScript, C++, all those languages that we probably did not learn in our own educational background. But it's also a force that is ready, willing and able, that has been done – has done an incredible amount of training over the past two years and works extremely well, as Deputy Assistant Secretary Hughes mentions, in a series of partnerships.

And so this is the force that we're building within the Department of Defense today. It's a very, very active force. It's a very, very capable force. But most importantly, it's a very, very professional force. And so this is the force that we will look to the future as we operate either in defense of the homeland, defending our own networks, or obviously in support of many combatant commands.

Jim?

MR. LEWIS: Great.

One of the words that's come up repeatedly is "partnership." And of course, many of you know that the first time we said public-private partnership was probably about 1998. So what I'd like to talk about a little bit – and maybe all the panelists can jump in – is, how do you know if that's working? How do you know if partnership's working? How do you measure it? And then how do you operationalize it? Like, it's nice to say we have a public partnership and we meet every quarter. How do you operationalize it? How do you know it's really working?

So I don't know who wants to go first on that one. I'm into metrics this month. Go ahead, Harvey.

MR. RISHIKOF: If you want. So, from the private specter's – private sector's perspective, the public-private sharing of information which Jim alluded to we've been working on since 1996 when we first – PV-62 (ph) and -63. For those of you who can remember, in the old Clinton administration we tried to do that.

The tall pole in the tent on this issue is the question of liability, because what the private sector is fearful of is putting forward information in which they become, instead of a victim, a target; that they have not fulfilled their obligations in compliance in some way. And since what we really want to know is all of the pinging, because the pinging has extraordinary information, we are working for the first time with DSS. And DSS is trying to figure out through their relationship with the defense industrial base, the DIB, how to get this information. But there's legislation currently talking about this issue of the sharing that everyone is concerned in the private sector, will we have some immunity if we share the information so that will be in the national interest without it coming back with either the FTC, the FCC coming and saying you have – or the SEC coming and saying you have violated some aspect and we're going to ping you. That's why it's been so hard over the last 20 years to get the private sector to share information with the government in a way that's effective would be my perspective to put out there for you.

MR. STOCKTON: I've got a metric to try out on you, Jim, and that is the number of personnel in the private sector, especially the owners and operators of critical infrastructure, who have security clearances. I'm on record, and Dr. Hamre knows this, of saying that far too many people in the Department of Defense have Secret and Top Secret Clearances. We got to drive that number down.

Flip side, though: if we're going to genuinely share actionable intelligence and threat data with those who are really on point to defend critical infrastructure, they've got to get access to classified information. We're not where we need to be yet.

MR. HUGHES: I was going to say not necessarily that it's something that you can measure, but I know that there's programs that DSS manages to do threat information sharing. There's programs that DHS manages to do threat information sharing. I think that, you know, given that DOD does not own, operate, manage 100 percent of our network and attack surface, we absolutely rely on partnerships with private industry to kind of be that first line of defense in a lot of instances. So it's an area we need to continue to collaborate on for collective defense.

GEN. NAKASONE: And I think at a tactical level for us, I measure it by, do we understand the key players that we're operating with? Because when I talk to my teams or I talk to my leadership, you know, rapidly we can tell how effective the partnership is, is when we understand who are the folks that we need to be working with closely.

The other piece that I would say is, do we understand the technical structure of those that we're going to support or are going to support us? The first time that we see a network is perhaps not when you want to see it in crisis. And so hopefully the metric is, is we've seen it before, we have a map to it, we understand the key terrain of it, we understand the challenges and opportunities that go with that.

MR. LEWIS: This might be a question more for our DOD and Cyber Command colleagues, but I know Paul and Harvey will want to chime in. But how has the relationship – and this is something Aaron kind of hinted at – how has the relationship between NSA and Cyber Command evolved, and how should it evolve in the future? What would you see it looking like three or four years from now when your NMTs are fully deployed and everything?

MR. HUGHES: I mean, I'd say very much right now it is a relationship out of necessity. I think the organizations share a lot of – share a lot of skills, share a lot of infrastructure. I don't – we are not at a point right now where we're going to look to separate Cyber Command from NSA, again, because there's – there is a high degree of synergy between how they're operating.

GEN NAKASONE: I guess I would say I would characterize it as being – and having seen it for a number of years – so it's a maturing relationship. What we looked at in 2010 on the 25th of May and stood up Cyber Command and thought about the partnership is different today in terms of what we as CYBERCOM are capable of doing. I think at the end of day we will always be focused on creating effects, and rightly so NSA is focused on foreign intelligence and information assurance. It's a rich partnership. We have to have that partnership. But I think, over time, I think as we have seen, is that we become increasingly more capable and our partnerships are important with NSA, just as they're important with the private sector, Defense Intelligence Agency and our allies.

MR. LEWIS: OK.

Paul, do you want to—

MR. STOCKTON: No.

MR. RISHIKOF: My question is, is we've talked a lot about does it make sense to have someone wearing a military uniform in charge of both of those agencies? And I think it's always well worth exploring what the role would be of having a civilian involved in that relationship. And part of it is trust-building, and part of it is sharing information which is critical in the area, and the notion that DOD we assume is going to have an offensive capability. That's their function, is projecting force. Whereas the attack issue of sharing what our vulnerabilities are is a little bit different, and we need to have a greater understanding of that because it's the private sector that they're looking for – as we say, it's the intellectual property that's the crown jewels that we have to protect for innovation. And how we build a system that does that may require a little bit more civilian input as opposed to a military – pure military perspective.

MR. LEWIS: One of the issues that's come up – and then I'm going to turn to you folks for questions – that's come up repeatedly, not only today but in other discussions, is the issue of thresholds, and what are the thresholds we're going to look at, both through the application of international law, for a decision on proportional response, and for deciding when the handoff from civilian to military occurs. So have you thought much, all of you, about thresholds?

I'm going to ask each of you, so don't think you can dodge this one. (Laughter.) I've thought a lot about thresholds, and what I've discovered in the places I work is there's no agreement, so – which is a good start.

Harvey, do you want to go first, or?

MR. RISHIKOF: So I brought a prop, because Justice Breyer always brings a prop when he talks about understanding how we rule and understand or organize our Constitution. You know, he goes in his pocket and he pulls out a small document and he goes, this is the Constitution, this is the operating procedure for the United States. And also it's a – (inaudible) – it's pretty easy.

This is what we've produced at DOD, being lawyers, our prop. (Laughter.) This is the Department of Defense Law of War Manual that's just been produced.

MR. LEWIS: And that's the executive summary. (Laughter.)

MR. RISHIKOF: And then I have the TALON manual for applying the Law of Armed Conflict to cyber. Then I have even more manuals that we've generated, all trying to deal with the threshold policy. Because in the end, my simple answer is the law is all about – how many lawyers do we have in the room? So it's – how many people can write an algorithm in the room? Raise your hand. OK, they're the real dangerous people in the room, as opposed to the lawyers. (Laughter.)

And though the threshold question is a legal issue to give authority and legitimization and justification for force, it ultimately will be a policy determination. The threshold is going to be a

political determination that allows us to use all the force that we have in our defense under either Article 51 of the United Nations or the traditional notion of self-defense. But that's why the threshold has been complicated, because if we tell this general this is the hard line and if there's a violation you must respond, that puts us in a situation that historically most policymakers don't like to be in. It's all about legitimization of policy. That's why the threshold's been hard.

MR. LEWIS: I would just note, though, that one of the problems – I agree with that approach, but one of the problems is that some of our opponents exploit the ambiguity there and try and do things that are harmful, but stay below the level they believe would provoke a response.

MR. RISHIKOF: Right. So we have a spectrum of cyber operations that we've put together. This is a JAG officer who's a wonderful guy named Brown. And it's all about what's an enabling operation and what's an attack. How do you classify the issue for the appropriate response? And that's why this – so how many people think the Stuxnet attack was an act of war? That was when we went – when whoever went after the centrifuges of the Iranian nuclear program. Was that an act of war?

MR. LEWIS: That's a trick question. (Laughter.)

MR. RISHIKOF: But you see why from a legal perspective, an international law perspective, this is a very hard issue for what allows you then to respond, if you have the legal justification why. It's the classic marriage of policy and law.

MR. LEWIS: And I won't politick, but it does, though, affect your ability to deter because if people are uncertain then it, I would say, may reduce deterrence. But go ahead.

MR. STOCKTON: Jim, I agree with that. I think that thresholds are a little bit like pornography: we're going to know it when we see it. We'll know that it's been crossed at that point. We need to develop plenty of options in order to be prepared for responses that are appropriate and not necessarily in the cyber realm.

But I would say this. As we think about deterrence and the development of response options, it's extremely unlikely that cyber warfare is going to come out of a bolt from the blue, surprise all-out attack on cyber systems. It's much more likely to occur in the context of an intensifying regional crisis in the South China Sea, in the Baltics, whichever region you'd like to pick. And we need to be prepared to understand the escalatory context in which the president will be looking at options and thinking about, well, which thresholds have been crossed in this intense political crisis, be prepared to operate in that context.

And let me just add, if you have an interest in this general realm of the context for decision-making you need to take a look at Jim Lewis' recent testimony to the House Foreign Affairs Committee. Jim, it's really, really useful.

MR. LEWIS: Thank you. They hated it, but – (laughs, laughter) –

MR. STOCKTON: Well, I was persuaded.

MR. LEWIS: (Laughs.)

GEN. NAKASONE: So, I mean, I think the threshold piece, as I listen to it and at one time had a policy job – and very, very pleased to be an operational commander now – (laughter) – I would say that what the nation is asking and what my boss is asking of me is, whenever that decision is made, have you formed the partnerships? Do you have the capabilities? And can you work, as Harvey talked about, within the authorities that are given you?

And that's where we're focusing our time right now. That is – that's the most important thing that we can do to deliver options, to think through how we're going to be able to respond when a decision is made. I think that's the right focus for us, and I think that's where we will continue to be, is figuring out what are those partnerships/capabilities and how do we operate within the authorities that are given us.

MR. LEWIS: Aaron?

MR. HUGHES: Yeah, and I would just say that, again, it's a case-by-case basis. I'll use an analogy different than pornography. Maybe I'll use a poker analogy: it's going to depend on the circumstance – (laughter) – and it's going to depend on, you know, some of the dimensions of the significant consequence threshold, right? Has there been damage to property? Has there been financial implications? And then our response is going to be a whole-of-government response.

You know, I think people have in their mind that if there is a cyber event on the United States that we need to respond in cyber. You know, as Sony showed, we responded through financial sanctions and otherwise. And I think that our response is not always public, but our response will always be or always take into consideration a whole-of-government approach, of which DOD and the tremendous professionals at Cyber Command will help to develop our cyber response options that our decision-makers will choose from.

MR. LEWIS: I have – I have loads of questions, but why don't we go around the room. There's two in the front here if we could get them. I think we need the mic. And then a third. We'll just pass it down the row.

Q: Hi. Scott Maucione with Federal News Radio.

This is for you, General. General Lynn from DISA said that the Joint Operational Headquarters for DODIN has been in seven named operations since it went into IOC in January. Where are you in being operational? And have you been in any operations, named operations or anything like that? And could you go a little bit into the difference in your authorities and responsibilities between Joint Force DODIN and the Cyber Mission Forces? Thank you.

GEN. NAKASONE: Great. So I did see General Lynn's comments, and Joint Force Headquarters DODIN, an incredibly great partner as they look at defensive cyberspace

operations for the DOD network – as you heard General McLaughlin talk, number-one priority for our secretary. And as we take a look at defending our DOD networks – and Joint Force DODIN has been involved in that – have we been involved as a Cyber National Mission Force? Let me take a step back and talk.

So our mission is that third mission that General McLaughlin talked about, is to ensure that we're prepared, if there are disruptive and destructive attacks against the nation, that we can operate. We have been in operations. And while I won't go into the specifics of what we've been doing, we have teams right now that are not only trained, capable, but have been in use. And so from my perspective, as we take a look at where we're going to operate, we always have to understand the defense of our own networks. We also have to have a capability upon which, you know, when called upon the nation, whether in defensive or offensive effects, the Cyber National Mission Force can generate them.

MR. LEWIS: OK. The next one. Great.

Q: Yeah. J.O. McFalls. I'm a contractor out at Fort Meade. I know Paul well.

But I have a question. The introduction that General McLaughlin had said we're going to talk about organizational structure and how we're organized to do these missions that we just talked about. And so the question is, those of us that work for you guys are very anxious to see this new effort that's going on in the Joint Chiefs of Staff to create Cyber Command as a standalone, unified, functional command. "So what?" is my question. Is that good? And if so, what does that change and when is it going to happen?

MR. LEWIS: Well, I'll start by saying Kevin in some ways is ideally positioned with this because he – for this because he started out as a space guy. And of course, we know that DOD experimented for years with separate command – joint command, sub-command. So I think we're – I think I would see it as a period of experimentation – that it looks like we've learned a little bit from the space effort, that we're making some good progress. But I'll ask the others to please join in on that.

MR. HUGHES: With respect to, I mean, it's something that's under consideration. So the Department of Defense is consistently evaluating the Unified Command Plan. There's been recommendations that the secretary has taken for consideration, but nothing has been finalized with respect to elevation of Cyber Command at this point. I think there's potential operational efficiencies and effectiveness that could be had from elevating Cyber Command, but that is something for the secretary to consider in his decision.

MR. LEWIS: Please just don't ask easy questions, by the way.

GEN. NAKASONE: I'll take that one for the record.

MR. LEWIS: Oh, OK. (Laughter.)

Q (?): Good.

MR. LEWIS: So we've got someone in the front there, in the red sweater. Stand by.

Q: Good morning. I'm Maggie Smith. I'm actually one of General Nakasone's cyber officers for the Army.

And my question is, from where I get to sit – usually I'm briefing you, sir, so I get to ask you a question now. Where I sit, we see a lot of attrition in terms of talent, and so talent management is a huge problem within the Army, within the DOD, but also within I'm sure the rest of government, as the private sector has more salary opportunities, as well as promotion for growth. So I was wondering how you feel about that as you move towards – as we all move towards FOC and the 2018 deadline for that, and what your thoughts are on that.

GEN. NAKASONE: So as Maggie mentions, one of the things that the services I think have done a very, very good job is recruit a tremendous amount of talent for our teams. This talent that has been recruited over the past couple years has come in, has been trained. And as with any service, you know, now we take a look at how well do we do at retention. I think the grades are still out on that. Each of the services does both recruiting, training, retention a little differently.

But here's what I think if I'm joining the force I would like to see. So first of all, I want to see some type of progression where I can operate in cyberspace and look out and say, hey, I want to be the next command master chief that leads Cyber National Mission Force, or I want to be Paul Nakasone someday, or some type of progression that gets me from the beginning to the end, where I can have a leadership capability. So this idea of having a professional force, incredibly important.

The second thing is, is that one of the things that we have done extremely well on is we have a fantastic mission. The mission doesn't change. The things that you can do in Cyber Command are different than you can do in the private sector and will always be different, I would say. And that is a selling point, particularly for a Millennial force that looks to serve. And I think that that's an important piece of it.

I think that there are certain, you know, enumeration capabilities that each of the services has to look at. So we pay for language capabilities, as many of you know – languages such as, you know, different foreign languages. We need to also think about paying for computer languages or special techniques, skills, capabilities that are very, very important.

And then I think the final piece of it is, as we take a look at it is, so, at the end of the day, what keeps most of us in service is some type of mentorship program, some type of, you know, involvement in the growth and professionalization of that force. And that's where each of the services has a distinct role to play, and we as leaders have a very, very important role to play.

MR. RISHIKOF: So I think you have to recognize – I call it – my son-in-law works for a small group called Google. So when you go to the Google campus or the Microsoft campus in Silicon Valley, it looks a little bit different than Fort Meade. (Laughter.) So this issue of how

you recruit the next generation – we were talking earlier – this is what we call the creation of the new cyber corps. And that's going to require universities to meet with the computer science programs, the law programs, the business programs to create a new generation of what I call the geek-wonk bridge so that we can actually have a corps of people.

And then we have to do a second thing. When I was growing up it was the Kennedy generation. We thought public service was important. So having some public service in these young people's world before they go out to the private sector to be paid a little bit more than even what generals are paid is a way of incentivizing and creating what the next gen has to be. And we need a not a whole-of – we really need to have the public/private sector education institutions banding together for a major effort to actually create what we need for the next generation.

And that's a big issue and that's a – that's what I would hope would be involved in the campaign issues going on, of a new perspective of what we need, because you're going to have a very difficult time competing for those MIT/Stanford students, given what they're being able to be offered if it's not public. And that's just – we have to recognize it and we have to have solutions for it because that's what we've done historically in order to make ourselves great.

MR. LEWIS: Aaron, I don't know if you wanted to jump in on that, wearing your In-Q-Tel hat, your old hat.

MR. HUGHES: Well, I guess I would comment on recruiting, and I think a larger issue is retaining the talent that is already in the mission force, right? So much goes into training them, in some cases from enlistment to being a certified operator. That process probably takes three and a half, four years. And so maybe we need to look at new policies that provide retention bonuses, like we do in the flying community, right, because I think that training cycle is a tremendous investment in time, money and energy; and to make sure that the teams that Paul is leading and the teams that the CPT and CMT commanders are leading – you know, have those capable operators and defenders is important. So I think retention is just as much as a key point as actually recruiting the folks.

In terms of, you know, my previous background from In-Q-Tel, I think there's areas where the government more broadly – not specifically CYBERCOM – needs to look at areas to partner with industry to bring in new, novel capabilities. And I think that the secretary has put a stake in the ground with his DIUX initiative out in Silicon Valley, and I think there's some burgeoning partnerships with In-Q-Tel and other innovative firms to try to – to try to cycle technologies through.

MR. LEWIS: Paul, did you want to add anything? No? OK.

I will say that my experience is it's a lot more fun to work for the government than the private sector, but it's just a personal point of view.

We have one in the middle there, the person with the blue tie.

Q: Hi. My name's Alec (sp). I'm with GW Center for Cyber and Homeland Security. Thank you for putting on this event. It's been really good.

My question is how – or what are the next major steps that we take to build a strategy to further develop and communicate a strategy of cyber deterrence that raises the costs on malicious actors, whether they be state or proxies of state governments or foreign terrorist organizations that actually deters?

MR. HUGHES: So, I mean, I'll take that. So much time, effort and energy went into drafting the existing strategy, we actually need to implement that strategy, right? And so if you think about the deterrent concepts that were articulated in the strategy released back in April, right – deterrence through denial; the secretary's number-one charge is making sure that we're defending our networks, defending our weapons systems and defending our data. We need to make sure that we're also resilient, so in the event that attacks are successful we can quickly bring those capabilities back online. The CPTs have done a tremendous job in responding to intrusions over the past year. And we articulated for the first time, right, that we want to build offensive capabilities, and making sure that those options are baked into the command plans that we use to fight in a variety of different domains.

So I think it's less of developing a new strategy and more in making sure that we execute and implement the current deterrence posture that we've defined in the existing one. And I think that will continue to evolve. I think sometimes we lose sight that CYBERCOM is both an operational command and is – and is also building the capabilities as we go, right? So we will get there. We will absolutely make sure that we have the appropriate options that can deter adversaries in cyberspace.

MR. RISHIKOF: So Paul mentioned, you know, pornography from Justice Stewart: you know it when you see it. And Justice Stewart always regretted having put that in lexicon because really, I think, as – I would say as a law clerk what the justice was really saying was that we had created a vocabulary of understanding and identifying the issue. Because in pornography we have a First Amendment problem, so you don't always really know when you see it. So this issue of actually having a vocabulary that nation-states would understand as to what the rules are.

So the first is cybercrime, Title 18. We are trying to actually make it effective. And I was talking to Ellen (sp), and supposedly the Chinese are saying, yes, these people are involved in cybercrime, we will give them up to you.

The rules for cyberespionage – espionage is as old as the Bible, the Old Testament. It's just something that nation-states do, and we sort of know the rules. So that's why Sony was a little bit different, because when you have a wipe-and-swipe that's not what you do, allegedly, in espionage, whereas OPM is classic forms of espionage.

And then cyberwar is, will we have a vocabulary of what you can do or not do? What's on the table, what's off the table when you use your cyber? That's what has to be done.

Now, when you deal with non-state actors it's a totally different perspective because they're not following the rules. But for the state actors, those three arenas – of us knowing it when you see it so that we have a vocabulary so we don't – mistakes – that's how you have, really, a strategy. Because it's not just us, as we always say at the National War College. The enemy gets a vote, too. So how they understand it is sort of significant, and that's what we have to evolve over the next short term, decade or so.

MR. STOCKTON: I think Aaron and his team are making terrific progress in the deterrence realm. I'd just like to add a little bit of spin to that, and that is we sometimes think that deterrence by denial as somehow separate and distinct from threats of retaliation. The two go hand in hand. We do not want to live in a glass house. The better prepared we are, the more resilient we are to be able to survive and reconstitute our ability to retaliate, the better off we're going to be and the more credible those threats of retaliation are going to be.

MR. LEWIS: Let me pool a little bit on the deterrence threat, because this is very much an internal discussion, a domestic discussion that we've had so far. And when you think about the folks we're trying to deter, some of them – the Iranian Revolutionary Guard, the General Reconnaissance Bureau in North Korea – not the most stable decision-makers, and perhaps not the most open to analytical influence. We have more serious opponents, too, in both China and Russia. How is it you think about miscalculation in this area, which may be the greatest problem in some ways for deterrence? And how is it you send a good deterrent message? What would a good deterrent message look like, that opponents would understand? And I say that with – having talked to three out of those four folks, I'm not sure they always get what we're saying.

MR. HUGHES: I think the policy is evolving. The escalation framework in cyber is not well-known. I think that – I'm not saying that it requires more study, but I think more dialogue around what that really means if you're – if you're to have, you know, additional attacks like we saw from Sony or in other instances. You know, I think that as we can hopefully communicate and evolve with the more stable adversaries and hopefully deny the non-state or less stable adversaries, maybe we can avoid getting to a further escalatory conflict.

MR. LEWIS: Great. Anyone else? That was a shade of Herman Kahn for a minute there.

MR. RISHIKOF: Well, you're in a unique position because you've been dealing with the GG Group (sp) quite dramatically, but I would say that when you – when you think of the origin of deterrence, it's always fun to look at it because Tom Schelling, who was one of the original thinkers of it for MAD – mutually assured destruction – and he still got a Nobel Prize – if you spoke to him, they believed when they actually constructed the doctrine that right about now we'd have about 25 or 30 nations that had nuclear power, that had weaponized. We've been so successful, beyond the originators' concept of what would happen.

So we're at the beginning of this dialogue. So we talk about open-kimono negotiations; if you do this, you know what we can do to you. When you think about it, the amount of destructive capability that cyber has, that it has not taken place is a demonstration that there is a sort of working norm that we've all sort of agreed to at this point who have that power, nation-

states. So it's one thing as in practice and how it will evolve with the doctrine and then will evolve to accepted theory, but currently there – if you actually look at what our abilities are and what hasn't happened, it's a very sort of good sign for the dialogue at a certain level.

MR. LEWIS: Let's get a few more questions from the audience. We've got one in the back right there. And remember to please identify yourself.

Q: Hi. I'm Joseph Sweiss. I'm with ML Strategies, and we represent some of the leading organizations that provide cybersecurity, certifications to departments like DOD.

DOD has some commendable efforts. There is Directive 8570, which provides certifications to various individuals and military personnel that are guaranteed IT and cybersecurity certifications. And it was so successful there's Directive 8140, which is expanding on that. So my question is, for other civilian agencies looking to implement IT and cybersecurity training and certifications, what lessons can be learned from DOD's development and implementation of these directives?

MR. LEWIS: You may have stumped the band with that one. (Laughter.)

Q: Sorry.

MR. RISHIKOF: I would say when you get into the weeds it's fine, but there's the ISO that is really international standards, and it's all about creating the standards trained to those standards. But at a certain level at this point in time, one of the givens is offense beats defense. And since offense beats defense, we can raise the game for a variety of areas. And then we also have a problem in this space, which are zero-D – defects. So you can have all the standards in the world, but if there's a problem in your code that has not been discovered yet and is exploited, that's the problem which we're involved with. Because that vulnerability in the code, the vulnerability in the hardware, and then what we call carbon units – you know them as people – people do things that are just not smart. And that, with all the standardization, how we get better at that is what we're looking for network defense.

So I think both the civilian and DOD understand that problem, and we're working and striving and able to create the atmosphere and frameworks that will be the most effective.

GEN. NAKASONE: So I might add. Let me just talk a little bit about training because this is what I would say we have learned. And if other agencies want to adopt it, that's great.

What have we learned in training? That there's one joint training standard. And when we started off with CYBERCOM, we were very, very specific to say that there was only going to be one joint standard, and it was going to make sure that all the services met that joint standard. So as an operational commander, a joint operational commander, when I get an Army team, a Navy team, a Marine team, I get the same type of trained team, foundational skills. Critically important. We learned that lesson from Special Operations forces and it has served us very well. And I think just in terms of what we've learned in training – and we have progressed rapidly in training – that has been a key lesson learned.

MR. HUGHES: I'd say that goes for the total force as well, right? Your Guard and Reserve folks are trained to the exact same standard, so.

MR. LEWIS: Great point.

We had some questions over on this time. Ooh, we got a bunch. Can we get the fellow in the back, and then we'll go to the –

Q: Hello. Patrick Stallings, congressional fellow – military congressional fellow.

When we're looking at the balance of authorities and privacy, particularly with the upcoming Cybersecurity Information Sharing Act, there's some concerns about backend scrubbing of private – of – or private identifiable information. From the Defense perspective, is there a need for real-time sharing of information across the whole of the government? Or is near-real-time sufficient? Or can a technical method be implemented, or would that undermine the intent of private-to-public sharing?

MR. HUGHES: Maybe I don't understand the question right. Is it that we need to share data between the government and private industry at net speed in order to defend our networks, or?

Q: At real-time, or is near-real-time sufficient? Because – is it necessary to share the information once it hits government at real-time across the whole of government, or is there time to scrub it for the private PII?

MR. HUGHES: You know, I hate to keep coming back to "it depends," right, to the nature of the threat. I think that the operations centers within DOD and the intel community are collaborating with the DHS NCCIC in the search to declassify when possible or to have the appropriate tear lines to share that information with the private sector. I'm not aware that that is done at net speed right now. But I know that in the event that we – if the government – the intelligence community or DOD was to identify a significant threat, we would absolutely partner with our law enforcement colleagues to get that information to the private sector as fast as possible.

MR. RISHIKOF: So the issue that we're confronting now is that we have multiple doors, and the position of the government is any door is a good door. You can go to the FBI. You can go to the Secret Service. You can go to DHS. You can go to NSD. You can go to certain elements in DOD. We have people here from the defense industrial base, at DSS. We know that's the door you're supposed to go through.

The second issue of your question, though, is the animization of the data is what we need in order to rack-and-stack and analyze the big data. That's where the really interesting issue is, how you animize the information for the public – the PII so that we can get a large aggregate and then start massaging it to find out correlations that are important. That's what your question really is. Yes, the first point is to get it, but the second point is how do you aggregate it and then

how do you bang it to give you the leverage you want out of the big data? That's the second big part. And that's really an issue that goes both to civilians and DOD, but also the private sector. And that's where the – quote, "the money is," is trying to figure out how to exploit that large data and then use it either for military purposes or for commercial purposes. That's where the world is going.

MR. LEWIS: Yeah, we had one more over there and then I was going to make a joke about information sharing. (Laughter.)

Q: Graham Jenkins with EY.

So it's good to hear about DHS/DSS cooperation with the defense industrial base, but I wondered to what extent do those agencies have powers of compulsion to insist on certain standards? As you say, all the standards in the world can't prevent some things from happening. And so at some point do low-level attacks that continue start to cascade into something more grievous and potentially damaging to our capabilities? And does that, in turn, have a knock-on effect on the larger economy at some point after that?

MR. HUGHES: Again, you know, speaking from a DOD perspective, I know that the undersecretary for AT&L, Frank Kendall, and DOD CIO Terry Halvorsen are working to make sure that acquisition law and some of those contracts define very specific cybersecurity standards so that we don't have the very basic kind of hygiene effects of, you know, poor security built into products or poor security on DIV networks. So they're absolutely looking at regulations that can help define what those standards are.

MR. LEWIS: Let me ask a question, though, which is that, what – I think at some point Paul mentioned Special Operations Command, and there's been a lot of discussion of that as a model for how Cyber Command might organize some of its work. How do you think that – is that useful to think of this in the context of Special Operations? And does that help – and this is a two-part question – does it help other combatant commanders think about how to incorporate cyber into their missions?

So I don't know if that's just – I think everyone could talk about that. But how do you – you have a new capability. How do you organize it? You guys have done a pretty good job. And then how do you get other combatants to build it in? You know, how do you get them to understand the new capability?

GEN. NAKASONE: Yeah, and I think that, you know, with the risk of any analogy, right, it's –

MR. LEWIS: Sure.

GEN. NAKASONE: – it can be shaped to what you're trying to drive towards.

There were some very, very interesting things that we looked at Special Operations Command, particularly as we looked at training, and said they really do that well, we want to be

able to leverage that. I think that that's a very, very good exemplar. The way that they function as a – you know, as a functional command, you know, perhaps maybe that's also something that Cyber Command in the future will look at.

But I think to your point of how do you get this into the combatant commands, you get it into the combatant commands with the planners, that are working where? In the J-3 and J-5 spaces. You have very, very good people at understanding capabilities and assessment in your J-8. When you move it to those domains and the culture becomes one of an operational culture, then you have success. Training those people, making sure they understand how we operate in the domain, how the domain can support their geographic combatant command? Now, that's the challenge.

MR. HUGHES: And General Nakasone is spot-on there. One of the roles of my office is to collaborate with those J directorates and the plans office in OSD to make sure that those combatant commanders understand what cyber can do for them, as well as what it – what it can't. You know, we have a lot of pilots and other operational folks that have come up in other operational domains that don't necessarily understand the capabilities, and we're trying to provide that level of translation and collaborate with CYBERCOM to make sure that those capabilities are baked into plans from the ground up, and not just slid in on the side once something is fully vetted.

MR. LEWIS: Paul, do you want to –

MR. STOCKTON: I think for many of the regional combatant commands it's fairly simple to draw lessons learned and adapt them to the cyber realm. Not for Northern Command, maybe not for Pacific Command. It's easy to imagine that in certain kinds of events Northern Command would be the supported command and you would bring these special capabilities to bear. We've seen some struggles with Northern Command incorporating Special Forces into their operations. That's been interesting. Maybe some of these challenges still remain to be examined for Northern Command, and parts of Pacific Command as well.

MR. RISHIKOF: So to me there's a macro and micro way of sort of thinking about the problem.

So the macro way is, when you think of Special Command – the Special Forces, what their missions are, they're very well-defined. They have a very clear, distinctive objective when you employ them.

And you think, at the micro level, we always taught that what makes the Special Operations forces so fascinating is that we say the problem defines the organizational structure. So if it's a kill mission with an assassin, everyone who supports that particular functionality. If it's a naval experience of blowing up a ship, the Navy guys who understand how to do that, they'll do that.

So that's the two big macro. And it always is a rice-bowl problem with DOD, and that rice-bowl problem Special Forces had to work through.

My issue is – with the analogy is it's an inverse relationship. Usually the younger person in the command understands cyber and the coding than maybe the three-star, and they're closer to that issue. So you want to drive down that capability to those individuals with the troops. Your problem is you want to make sure that the unintended consequences of having those troops or machines responding are fully understood at the policy level. That's what makes it complicated for the facile analogy.

The analogy is powerful – which, I want to know, when I look at this person and they are a cyber X, I'll know exactly what languages they're trained in, I'll know exactly what their experience is. The same way, when I look at a Special Force, I know what their shooting capability is, I know what their swimming capability is, I know exactly what they've been trained to do, so they become interoperable. That's what you're looking for for the training. But the consequence is, is as we move into the Internet of Things, what you think you're doing vis-à-vis the response may be a little bit more complicated and have consequences you haven't thought through. And you want senior policymakers in that – in that dialogue and in that algorithm.

MR. LEWIS: Harvey said you have enlisted personnel who know how to code and three-stars who don't. I was going to ask him where two-stars fall in that range, but – (laughter) –

GEN. NAKASONE: Well, they're the heart of the force, obviously.

MR. LEWIS: Maybe we'll skip that one. (Laughter.)

A couple more questions. We have one in the front up here. (Laughs.)

Q: Hi. Sydney Freedberg, Breaking Defense.

A question for the general in particular, but for I think the whole panel. One of the other things that's always interesting about SOCOM, that we were just discussing, is it has its own relatively small but widely admired acquisition outfit. It actually breaks down a lot of the barriers that, you know, mean that, gee, today I want to get a pencil sharpener, 15 years later I have one that weighs five tons. And there are some revisions even in the current NDAA that would give additional authority to CYBERCOM, although I don't profess to understand a single sentence of them. So especially given the rapid pace – you know, the Moore's Law-plus pace at which the software and the hardware are evolving in this world – how does CYBERCOM need to break out of the current acquisition structure? And to what extent are new authorities or new regulations part of that solution?

MR. HUGHES: I think you hit it spot on, we need to be more nimble, right? I mean, coming from, you know, a firm like In-Q-Tel, where we saw innovating happening on a very rapid pace, I know that CYBERCOM could take advantage of a lot of things that commercial industry are developing. I think there's also areas where private contractors that are doing kind of exquisite development work is also very relevant to some of their mission space. So I don't think we can go from zero to 100 immediately, but I think some sort of pilot or trial that provides

Cyber Command with those exquisite acquisition authorities might be – might be relevant, and we could potentially see that in the coming years.

GEN. NAKASONE: Yeah, and I think closer to the problem set, as they work the policy pieces out – and, you know, whether or not U.S. Cyber Command is elevated or not, obviously another topic – but for us at the – at the cutting edge, for our teams, we have developers on our teams. And so where are we focusing our developers? We're focusing our developers with the people that have, you know, the exquisite information. Whether or not that's with, you know, the intelligence community or another government agency or it's with the private sector, that's where we want them to be, and we want them to understand it. And I think that's the important piece for us, is making sure that that partnership is wide and that we understand that's going on in all of those sectors.

Q: So people are building a lot of your software in-house, it sounds to me.

GEN. NAKASONE: So we have developers, and we have developers that are helping us develop our effects, yeah.

MR. RISHIKOF: But you have – you have two great models: you have In-Q-Tel and you have DARPA. And the exploitation of those vehicles for test beds would be something – and Secretary Carter fully understands that. He has a real grasp with these issues. And building out that flexibility because the military mind is – by nature has to be conservative because people die if they're wrong. So that usually results in a little bit more less Silicon Valley "let's give this a shot and see if it happens." And I'm with Crowell & Moring. I spend a lot of time with the new startups trying to find funding, and some works and some doesn't work. But the idea that using the current vehicles we have – In-Q-Tel and DARPA – and blowing them out as test beds, that's a great model for being able to tap what's happening on the innovative level. I see some people are shaking their heads no, but that's a way of thinking through the process.

MR. LEWIS: We're getting close to the end. I see two hands over there and then I've got a final question for the group. Why don't we do the one in the front and then the one – well, actually, why don't we do the one in the back, because they're closer to you. Thank you.

Q: Thank you. My name is Hermes Levi. I'm for OWS.

My question is about, it seems that there is a drift toward the computers and a little bit we forgot the human mind, which is much more powerful if the faculty are used. Have you ever envisioned a program or a dimension where you can look up at this subject, how to develop the human mind and we counteract a little bit the computer? Because it might be much more helpful. Have you explored this dimension?

MR. LEWIS: Well, I think there are some DARPA programs. I know there are some programs in other countries that are looking at this, and some of the university research. There's some neat stuff. I keep waiting to see it come a little bit more to fruition. Right now the most public face of it is the wearable device, and that's a way to enhance your performance, enhance

your thinking. We're just at the tip of this, though, so it's a very early stage in terms of both R&D and certainly in deployment.

And you know, I for one cannot afford an Apple Watch, so that's going to limit my participation for a while.

We had one in the front, and then maybe we'll – go ahead.

Q: Thanks. Patrick Tucker, Defense One.

This is for General Nakasone. Earlier we were talking about all of the different lengths that the DOD is going through to stand up these teams in terms of training, and particularly the big exercises. And we also talked about the really Byzantine legal structure that would govern how offensive cyber effects were deployed. And I wonder if you can touch on how that Byzantine legal framework would affect training if soldiers are going to be given a variety of different authorities to have cyber effects. And also – you probably can't answer this – have you developed any insight into the way other state actors stand up their own cyber commands, how they train or conduct these sort of exercises?

GEN. NAKASONE: So I'll take the first part and stay on the first part. (Laughter.)

When we take a look at effects generation, whichever we're going to do – offense or defensive – the most – the most impactful way that we've learned to be able to generate those effects is in a training environment.

And what does a training environment look like? The training environment looks something like this. You first of all have a capability to replicate the network that you're looking to either defend or attack.

Secondly, you're going to have a thinking opposing force that can offer your teams challenges and a number of different means where they have to think through what they're going to do.

The third thing you have to have is you have to have a scenario that's realistic. I would tell you that, working with the folks that are coding, that they will immediately call you when the scenario does not look realistic or does not replicate what they see in the real world.

And the last part, the most important part that we've learned in every single domain, is you have to have an assessor, someone that can provide you the capability to say this is what you did well, this is where you fell short, and this is the standard that you have to achieve.

And so those are the elements that we've been working towards building, exercising and training towards as we take a look at a number of different adversaries. And from our perspective, I think it's generated a lot of capability for our teams.

MR. LEWIS: Great.

I'll wrap up with a final question, then, which I'd like each of the panelists to respond to and I may push back on them a little bit. But this event is about homeland defense and DOD's role in homeland defense, and it's October and Cyber Security Month for what that's worth. Tell us what your priorities are for homeland defense and what you think the nation's priorities should be as we build homeland defense in cyberspace.

Aaron, do you want to start?

MR. HUGHES: Sure. I mean, I'm happy to start.

I think General McLaughlin did a great job at articulating what DOD's role is. You know, first and foremost it's that indications and warning of significant events that might affect the homeland in cyber. Cyber Command is out there in red and gray space, determining what attacks might come against our networks, and we're doing our absolute best to defend against those.

In the event that something is successful, DHS has the primacy for that mission, along with FBI in an investigative capacity. As resources are stretched thin, we have a well-defined DSCA process – Defense Support to Civil Authorities – with which Homeland Security, with which FBI can pull from DOD Title 10 forces to provide a wide range of technical support, response capabilities, et cetera. So, you know, I feel like it's a well-defined paradigm for how DOD plays in that, but we're absolutely contributing to defense of the homeland. It's very much a whole-of-government approach to cybersecurity.

MR. LEWIS: Well, for a new guy he really knows his portfolio. (Laughter.)

Paul?

GEN. NAKASONE: So, for us, as we take a look at defense of the nation, we're focused on three elements. First of all, how do we build the right partnerships, robust partnerships, the partnerships that are going to matter in times of crisis? Secondly, the capabilities that we need to develop to ensure that we're able to mitigate or stop and disrupt a destructive attack against the nation. And thirdly, to – again, to Harvey's point, the authorities upon which we operate – making sure we fundamentally understand those authorities upon which we're going to operate and the authorities we need to operate in.

In terms of your second question, what do we need to do as a nation as we think about it, think of this. The nation, as we take a look within the government, the largest capacity for defensive capabilities rests within DOD. And I think we have to think through what's the most effective manner in times of crisis that we're able to provide support to another federal agency, much as we do as Secretary Hughes here says with regards to DSCA, in a very, very rapid manner.

MR. STOCKTON: I used to commit acts of DSCA.

MR. HUGHES: Mmm hmm. Absolutely.

MR. STOCKTON: And Sandy, for example, provided very harsh lessons learned for how operations actually need to go forward in Defense support to the Department of Homeland Security, for example. But in Sandy, we had the benefit of decades of experience with natural hazards. We have been able to, above all, build a concept of unity of effort that provided for integration across National Guard and Title 10 forces, and collaboration with lead federal agencies.

Folks, that is not going to happen in the cyber world. The very first time that a large-scale cyberattack occurs on the United States, we will have had to have relied on exercises like Cyber Guard in order to understand what is coming. That is an immense challenge.

MR. LEWIS: We did an exercise here on responding to a crisis with senior policymakers or people who had been senior policymakers, and it turned into what people might call L-I-C, LIC: lawyer-intensive conflict. (Laughter.) Because that's exactly right, is when you say, OK, what can we do, it turns out to be hard and undefined.

MR. RISHIKOF: So there's always the lawyer-bashing part of the panel. So what you call Byzantine I call the law. (Laughter.) And what Justice Brennan used to say, there are all these technicalities: you know, it's called the Bill of Rights.

We have dot-mil. We have dot-gov. We have dot-com. You were very articulate in understanding that the primary mission of the military is to defend the military network. Their secondary mission is dot-gov, which is actually DHS's issue. And the issue there is, do you think DHS has the capacity? I love Jeh Johnson. He's doing a great job. They maybe have a thousand people, FTE, they're building up to it. I go to Silicon Valley and I sit down with Google and Microsoft, they believe that they actually have a greater capacity for coding and ability than the government does. That's the big issue, who has the appropriate mission?

So I went back in the private sector because we used to go around the country saying the battle's moved from the war room to the board room. The board room is the front line now of this cyber issue for the commercial side of intellectual property. The critical infrastructure issue is what our values are in maintaining that system. That's a different issue.

And so how we – this is why it's been hard, is because the range of authorities, the range of vulnerabilities, and who really has that capacity to be able to, quote, "defend the homeland" is still a little bit of a question mark. We know how good we are at what we can do. We also know how good our adversaries are. The issue of the virtual world and the real world is eroding. Our authorities are built on the ocean of the real world, not the virtual. That's why this has been hard.

But in the end, it's going to be how we do this with a sense of authority and legitimacy, and under law, which will be – what has always been our hallmark for the long-term gain and not the short-term response. That's how we have to conceive of the problem.

MR. LEWIS: We started talking about this here in 2011 with General Alexander, and at that point the first question we posed in a very similar setting was, if NORAD can defend our airspace, why can't Cyber Command defend us in cyberspace? And I'm not going to ask the panelists to answer that one. I will say that it gets to Paul's point about analogies and where they don't always work.

We have gone down the path. We're much further along than we were in 2011. It's not necessarily the air defense path, but it is a path that seems to be working. And I appreciate everyone coming out today and giving us a little insight into it, particularly Aaron and Paul, of course Paul and Harvey as well. So please join me in thanking an excellent panel. (Applause.)

(END)