CYBERCOM MEDIA ROUNDTABLE

May 7, 2019

MR. LUBER: Welcome, everybody. Glad that you could make it here today. Before we begin, how about we just go around the room real quick and do some quick introductions?

MR. VOLZ: Oh, yeah. Dustin Volz with the Wall Street Journal.

MR. BING: Chris Bing Reuters.

MR. LUBER: Okay.

MR. BARNES: Julian Barnes, New York Times.

MR. LUBER: Nice to meet you.

MR. MATISHAK: Martin Matishak, Politico.

MR. LOPEZ: Todd Lopez, DoD News.

MR. POMERLEAU: Hi, Mark Pomerleau with Fifth Domain.

MR. LUBER: Okay.

MR. HANNIGAN: Joe Hannigan, Time Magazine.

MR. LUBER: Okay, terrific.

MS. VAVRA: Shannon Vavra, CyberScoop.

MS. NAKASHIMA: Ellen Nakashima with The Washington Post.

MR. LUBER: All right, and you got some –

MODERATOR: Yeah. Welcome, everyone again, and thank you for your time today. I just wanted to briefly go over our ground rules. This is, as you know, on the record, and we are going to start with come opening comments from our leadership here, so we would ask that you hold your questions until after they're done. And for question and answer, in the interest of fairness and time, we'll do a round robin, you know, perhaps starting with Dustin and just going around and we'll keep going around, and we would ask that you refrain from follow-ups to the extent possible so that everyone has a chance to ask questions.

I think you've all gotten the folders – yes – that have some of the bios and useful information for reference. And again, we are grateful for your time today. And with that, over to you, Mr. Luber.

MR. LUBER: Okay. Thank you so much. Well, welcome again. My name is Dave Luber. I am an NSA senior executive assigned to United States Cyber Command as the executive director of United States Cyber Command. So, I work for General Nakasone, and I'd like to talk quickly today, first about our mission.

The commander of U.S. Cyber Command has the mission to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic international partners. During the past year, we've made a great deal of progress.

First off, we were elevated to a unified combatant command. In fact, on the 4th of May was our first anniversary as a full unified command, so we're really happy about that. We've also deepened our partnership alongside the National Security Agency and with – thanks to Congress with the passing of FY19 NDAA, there has been some new authorities that we are also very happy about for the Command, as well as some changes in Presidential Policy. And lastly, through the outstanding teamwork across the DoD, the U.S. government, and industry, we've made progress as a command in that area of collaboration.

So, let me go into just some basic history about United States Cyber Command. First off, in 2009, we stood up as a subunified command under United States Strategic Command, and in 2010, we said we are a FOC as a subunified command. And then if you jump ahead to 2013, we started the billet of our Cyber Mission Force. That's an important part of our mission is our people and the Cyber Mission Force as the people that make up United States Cyber Command.

And in 2018, as I mentioned, we were elevated to a unified command, and our Cyber Mission Force went FOC. So, just in the last year, Cyber Mission Force going FOC, having that elevation.

Another major event that happened for us in 2018 was the standup of the Russia Small Group. It brought together the best of NSA and Cyber Command to support a whole of government to safeguard the 2018 midterm elections. Now, I would love to talk to you about all the details of the Russia Small Group, but Major General Select Tim HAUGH is going to discuss that more later in the interview.

In the fall of 2018, we opened up our DreamPort facility in Columbia, Maryland, and if you don't know about DreamPort, we're going to discuss it a little bit more as we go on, but it's a combination of a state-of-the-art facility, innovative programs, and imaginative

people working together to find the next unparalleled capability for U.S. Cyber Command and the warfighters at large – writ large.

I've had the opportunity to tour this facility. In a few minutes, I'm going to actually give you some insights into some of the work that's going on there, some of the projects that we have ongoing, and how the outreach is working with industry and academia.

Also, since elevation in March of 2019, we conducted Cyber Lightning. This is a command post exercise in an unnamed area of operation, allows us to test, challenge, and integrate our cyberspace systems and cyberspace planning into global operations to support our joint force and combatant commanders.

Another key milestone –and you'll see some of these signs that we have up here, and we're going to reference some of these in just a moment - is the development of our persistent engagement strategy. So let's talk about persistent engagement for a second.

In the face of cyber threats, we have adjusted our strategic vision to one of persistent engagement with a persistent force. So let me explain. No longer reactive, but actually working in cyberspace in an area where there really is no sanctuary or operational pause. It is the center of strategic rivalry, and it is in this era of renewed power competition.

So, in essence what we're talking about here is persistent engagement as a concept where we are in constant contact with our adversaries, and success is determined on how we enable and act. And we'll talk a little bit more about that in the Russia Small Group discussion about enabling and acting.

Persistent engagement is also bolstered by persistent presence and persistent innovation. So in persistent presence, we share information to enable our partners to continually seek to – to partner continuously and not just to respond to incidents, but also identify and counter threats as they emerge in cyberspace, and also provide indications and warning to our partners.

Innovation. Cyberspace is under constant change, so we must innovate as a command, we must innovate as government, and we must innovate with our partners. So, persistent innovation is that part where we are working together, and I'm going to talk to you a bit more about that as I go into the DreamPort discussion in just a minute.

I also want to talk to you about community outreach and academic engagement. An important part of our success story is over the last year. Just locally here, working with Fort Meade High School, we have the CyberPatriot STEM program. Working closely with the next generation of our cyber work force is very important, and we want to help make sure that those students get a great introduction to cyber defense and to demystify some the cyberspace activities so that they can get a good start in their career in cyber.

We also have a partnership with over 50 universities across the nation and, you know, that type of collaboration allows us to leverage insights from those universities, participate with them in academic research, also spot talent for the Command and for the rest of the government, and also work on a variety of innovation projects with the universities. So, that's a, you know, really, I've been working in the academic outreach area for a number of years and it's an important part of our strategy, and we're actually out there working with those universities today.

So, let me talk about DreamPort. I'm really excited to talk to you about this particular facility. Again, it's over in Columbia, Maryland, and if you want to check out some of the work that's going on just on the internet with DreamPort, just go to dreamport.tech, that's t-e-c-h, and you'll be able to see some of the activities and some of the data calls that we have out there for some of the projects that we have ongoing.

But what I want you to think about is innovation, collaboration, and a facility where we can prototype concepts together between government, industry, and academia. So, this all is unclassified work and its surrounding – it surrounds a variety of problem-solving events to support United States Cyber Command. And as I mentioned, it's a place for Cyber Command, industry, and academia to team together.

So, we're also committed to reaching out to the community at DreamPort as well. We have opportunities for some of our middle school students around the area, high school, and higher education students to work on various projects over at DreamPort along with our Cyber Command professionals. It's designed to be a very collaborative space; lots of technology, work benches, and work and rooms where you can actually innovate together as a team.

It also is very adaptable. So, you know, if a particular project comes in, it's a large project, we can work the larger projects. If it's a smaller project, we use a small room just to have a breakout session for a short period of time. And if I could give you some sense of how many teaming events we could have ongoing at one time, we could have as many as 30 events going on at one given –at one time over at the DreamPort facility.

So, let me talk to you about some of those accomplishments. So, first off, we've had four rapid prototyping events, and these were public calls for innovators to gather and rapidly prototype solutions for pre-prescribed challenges that we had for the Command. Not only did we see success in those areas, but those four rapid prototyping events led to four different contracts with industry, and, in particular, one of those contracts was a single-person company. So not only is it big companies coming and working with us. It's also small companies coming and working with us.

And what we're really interested in are those innovative ideas. How can we get at some of those problems that are facing the Command, some of those opportunities facing the

Command, and bring the best and the brightest together in one facility to help us work on some of those issues?

We've hosted over 6,000 visitors over to the facility, and we've also partnered with the Office of Secretary of Defense, Small Businesses and Manufacturing to help protect small businesses in the DIB, Defense Industrial Base.

The one thing I really want to talk to you about, though, that's going on over in DreamPort right now, is a prototyping event that we have going on with zero trust networks. So, zero trust networks, if you're not familiar with the old models of doing cybersecurity, you might think of perimeter security, perimeter-based security, security in end points, networks, firewalls. But in some cases, those sorts of concepts were limited in their ability to identify insiders and also credential-based threats.

So what we've done is taken on this concept of prototyping a zero-trust network for – and this can be applied to unclassified networks, classified networks, but really what you're talking about is you look at your network in a way that says, "Never trust anything in the network, and always verify." And what I mean by that is that at the user level, at the hardware level, and at the location, you're always verifying that that particular user, piece of machinery, and location is actually authorized to be on that network.

So, you'll see things on the internet about micro segmentation, granular parameters – perimeters, and verifying user data and locations, but what I want to tell you is that we've brought together U.S. Cyber Command, the National Security Agency, and many different other industry partners to work on a zero trust concept for the Department of Defense. So, we're still in prototype phase, but I'm really excited about the progress we're making in that particular event going on over in DreamPort.

Well, I'll stop here, but before I transition to Major General Glavy, I want to leave you with a couple of thoughts.

Here at U.S. Cyber Command, the National Security Agency is our most important partner. The strength of the relationship will remain critical to the defense of the nation. NSA has world-class expertise, technical capabilities, and accesses that are crucial to United States Cyber Command's success. The United States Cyber Command and NSA relationship is mutually beneficial. The speed, agility in joint operations to defend last fall's election is one of the great examples, and General HAUGH's going to talk about that later on.

So, with that, I'm going to turn it over to Major General Glavy.

MAJOR GENERAL GLAVY: Thanks

MR. LUBER: And he's going to talk about JTF-Ares.

MAJOR GENERAL GLAVY: So, thanks again. Gerry Glavy, commander of the U.S. Marine Corps Force's Cyberspace Command and Joint Task Force Ares. I assumed command of Joint Task Force Ares in September of 2018 from Army Cyber Command. Of course, General Nakasone was a prior commander of Ares, so he's obviously kept a close eye on us.

The Command stood up in support of U.S. Central Command, very specifically in support of Operation Inherent Resolve, which we continue to support to this day. As the transition was made, General Nakasone also thought it was important to expand that mission set. The Marine Corps has a natural relationship with Special Operations Command and, of course, Special Operations Command also has a global VEO mission. So we were given the transregional global violent extremist organization mission to counter in cyberspace which we continue to do along with our support to Central Command and Operation Inherent Resolve.

What I've learned in these last seven months is three very important things. One is the ability for Cyber Effects to support a ground scheme, a maneuver. It's been impactful to execute in that manner very closely with obviously the commander forward.

Two, Mr. Luber mentioned it, but persistent engagement. So in this domain, you know, cyber's not a sometime thing; it's an all the time thing. So, literally 24/7, we are obviously in support of a forces forward, but this is a mission that requires a persistence day in and day out.

And then lastly, and probably most importantly, is partnerships. It's also a team sport. Very important how close we work with the intelligence community that the inner agency and certainly all our coalition partners is really how we gain a asymmetric advantage in the domain.

And with that, I'll turn it over to my good friend, Karl Gingrich from the J-8. Karl.

GENERAL GINGRICH: Good morning. I'm Karl Gingrich. I am the director of Capability and Resource Integration, also known as the J-8 for those of you familiar with the normal or typical staff structure. I just have three brief areas I want to talk on to kind of frame out any future questions following our opening statements.

USCYBERCOM has requested $592 million in our Fiscal Year '20 President's budget request. That's a matter of public record. It's out there in our justification materials in explicit level of detail. I'm not going to go into a whole lot of detail on the line items. Like I said, that's available.

That's a small portion of the overall DoD cyberspace activity budget, which is also available in the public domain as part of the justification materials. That measures about $9.6 billion in Fiscal Year '20 in the current request, so we're about 6 percent of that. So,

for 6 percent, the Department of Defense and the nation is getting quite a bit of capability and capacity from USCYBERCOM.

Broadly, I'll talk about it in two pieces, about $240 million is for the headquarters. Really, the headquarters manpower, headquarters IT facility, security, et cetera. The balance of it, about roughly $350 million goes towards support to the CMF, Cyber Mission Forces, as well as capability development. And that's one of the key authorities that really distinguishes us from some of the other combatant commands is General Nakasone's ability to develop and acquire capabilities, and I'll talk specifically about acquisition authority here in just a minute.

But how are we driving the Department? How are we ensuring that we are being effective in developing cyber capabilities across the entire Department of Defense? How are we ensuring that we are being efficient and good stewards of taxpayer money by reducing redundancies?

I'm really proud that the Command as, really as a sign of maturity, has established the Joint Cyber Warfighting Architecture. The architecture itself is classified, but it's really an overview of how we frame out our cyber architecture. Now, you'll notice I didn't call it a platform because you can't buy one, okay? You cannot buy one just because of what Mr. Luber talked about.

We need to constantly innovate in this space and our adversary gets a vote. So the way our adversary fights and approaches us and uses cyberspace, we have to be adaptable to that. We are going to change the way we fight. We are a learning organization across the Department of Defense and the Cyber Mission Force, so we have to have an architecture that is capable of allowing us to innovate and go where we need to go.

And then finally, I'm preaching to the choir here, technology. We're all about technology, and what we don't want to do is lock ourselves into, sort of, antiquated technology that then drives how we do business in the cyber domain.

So, you know, broadly, the architecture really provides a framework so that we can talk to senior leaders within the Department of Defense. It's also been very helpful in talking to Congress, to help them who are not, you know, deep in cyber every day, really to help them understand the context with which we are making our investments, where are our gaps, et cetera.

And so the architecture really talks about everything from our access platforms where we gain access to the internet, our tools that we use in cyberspace. We have a persistent cyber training environment that we are developing so that our teams can do collective training and mission rehearsal, as well as the censoring on the defensive side, as well as data management and command and control. So, that's broadly what the Joint Cyber Warfighting Architecture is.

The last thing I'll touch on is acquisition authority. To allow General Nakasone to acquire the capabilities he needs, Congress has given us a $75 million annual acquisition cap and we are executing that cap. Right now, we are currently on the right path. We're at $43 million in FY18, where we've used our own command acquisition authority, and we think we're going to approach the $75 million this year. That is due to sunset in 2025 right now. Okay. We got it extended into 2025. And we're also continuing to negotiate and work with Congress and the Department of Defense to see if we need to adjust that upwards, again, as a sign of maturity. Don't give us too much acquisition authority, let's just keep making sure that the ceiling is there so it doesn't limit us from doing multi-year acquisitions so that we can actually meet the needs of our Cyber Mission Force through innovative acquisition and capability development.

With that, I'm going to pass it off to Major General Select Tim Haugh, the Cyber National Mission Force commander.

MAJOR GENERAL SELECT HAUGH: Good morning. Tim Haugh. I also command an organization that was previously commanded by General Nakasone, so he's very familiar with Cyber National Mission Force. Role and mission of CNMF is we are focused on adversary malicious cyber actors, so the adversaries' hackers, that are targeting the critical instruction of the United States or Department of Defense networks.

We've organized our force into task forces that are aligned against the competitors in the National Defense Strategy. Plus, we have a task force that is aligned to our partnership with DHS. They're a critical partner, obviously the lead for the nation in terms of the protection of critical infrastructure, so we have been working very closely with DHS as we build out and as we've matured as a force.

From the CNMS perspective, we're one of the lead elements for General Nakasone that is working persistent engagement. When you look at the strategy that General Nakasone has laid out to compete in this space against the adversaries' malicious cyber actors, we've got to be out there every day, and we have to be in contact with them. That is – and we view that through his lens of describing things as the amount of resources we're applying to enable our partner, in this case, largely our domestic inter-agency partners in DHS and FBI, and then be prepared to act. Whether that's acting by being in their networks or being forward in areas that they care about. And we'll – I'll give you some specific examples of how we've approached that.

Big picture, here's how we've organized our persistent engagement campaigns. We've identified for each of our task forces three lines of effort. First line of effort is to gain insight into our adversary. Understand what they're doing, what they care about, and what they're targeting, and be prepared to share that with all of our partners.

The second line of effort is to enable defense, and that can be defense of our allies' networks, it can be defense of the Department of Defense network, or critical

infrastructure that we identify an adversary to be targeting. And then the third line of effort is really that act component. Be prepared to impose costs and generate options if the Department asks for those options. But we need to always be thinking about that in terms of potential threats to our critical infrastructure.

Now, more specific examples. In last fall, the Secretary of DHS and the Secretary of Defense signed a memorandum of agreement of the partnership between DHS and DoD as to how the Department of Defense supports DHS' efforts to protect critical infrastructure. And we started to outline within the Department how we could build some pathfinder activities with DHS so that we can learn together. As the capacity in the Department grows to be able to counter these malicious threats, how can that be brought to better defend the critical infrastructure. And we do that in lockstep with DHS.

The first two areas that we – that DHS chose to use as partnered activities, one was within the financial sector. So, this is now a partnership between DHS, Treasury, and then with specific – with the sector. And the goal there is for us to be able to identify outside of the United States any threats, and then be able to pass that information as quickly as we can to DHS and Treasury to be able to get that to the sector.

We're building a similar set of partnerships with the Department of Energy and DHS on an energy pathfinder, and for these, these are areas for us to learn together. How do we bring our capacity to bear to execute the missions we've been assigned, but do it in a very complimentary way with DHS, who's clearly the lead for the protection of critical infrastructure. So, that's the big picture of how we've organized, and then the partnership with DHS.

We've also started to do some initiatives based off of the changes in the law that Mr. Luber identified, which is now to press into persistent engagement. We've sent defensive teams forward to be able to operate in foreign networks. The purpose of that was to go where our adversaries are operating. To help or work with the geographic combatant commands so that they can grow partnerships, but also for us to be able to discover adversary activity to be able to make sure that our partners are aware of that, and then also to look at that from our perspective of, "How can we leverage that understanding to put pressure on these adversaries?"

The first round of those were really successful. As General Nakasone talked about in his testimony, we view that as really a good way for us at low costs to gain a deep understanding of how our adversaries are operating, but also to just raise cost for them in some of our – and also simultaneously protect some of our allies as we go forward. That, as a by-product, is one of the sources that we've used to also, in the conduct of our operations, identify adversary activity and then share that directly with industry. We've done that by leveraging VirusTotal, which is a platform for sharing of malicious activity. We've taken malware that we found on –in the conduct of our operations, and we've

posted it directly to VirusTotal with the goal of allowing industry, then, to quickly build countermeasures so that we are sharing that.

And we think that is going to be an area that we are going to continue to work with DHS and with –within the department as to what is the right method for us to do that. We started with VirusTotal because that was really an industry standard. But we really are looking for what are the best outlets to get information directly to industry so it will allow for critical infrastructure in defense. And we are having that discussion with DHS.

The other real clear area, I think, from General Nakasone's perspective that we're really proud of is the work that NSA and Cyber Command did as part of the elections. And this really was about a partnership between NSA and Cyber Command and then being good teammates with all of our interagency partners so that as we received very clear guidance from the Secretary of Defense about the priority of the defense in the midterm elections, and we really emphasized between NSA and Cyber Command how can we generate insights for DHS to be able to work with the states to pass that information so that we had a clear understanding of any threats from a cybersecurity standpoint, and then also with the FBI, that if we were able to uncover anything that was associated with (inaudible) influence, rapidly passing that to the FBI. Both of those organizations, DHS and FBI, were really good teammates.

But I think what we also saw is General Nakasone's vision of how to create speed and agility by the partnership between NSA and Cyber Command, allowing both of our missions to be more successful because of that partnership and how we work together. There are a lot of lessons that we learned in terms of information-sharing, how we can partner with DHS and FBI, and that really has set a foundation for us as we look to 2020, which will certainly be an area where we continue to grow the partnership with DHS and with FBI and across the industry to make sure that the nation's –we are doing our part in that role to defend our electoral process.

With that, turn it back over to Joe and welcome any questions.

MODERATOR: All right. Thank you, gentlemen. And, as I said, we'll –we've got ample time here, so we'll go around the room, and we'll start with Dustin. If you just go one at a time and circle around and thank you very much.

QUESTION: Okay. Thanks again for doing this. I really do appreciate it. I guess just to start, since, you know, we've heard so much about the importance of the partnership with –between Cyber Command and NSA, could you just give us sort of an update on where things stand in terms of NSA Cyber Command, you know, the separation? What does that look like right now?

MR. LUBER: Sure. I'll take on that question. First off, I can confirm you –confirm for you that General Nakasone has completed his 90-day assessment on the status of the

Dual-Hat Agreement. He provided that information to the Secretary of Defense and the chairman of Joint Chiefs of Staff for their review. And, of course, you know, it's in their lane, then, to make that decision. But I'll tell you, as we continue to work together, we see great progress in our partnership between United States Cyber Command and the National Security Agency.

As Tim points out from the Russia small group, we are learning as we go along but it is a great partnership.

MODERATOR: Chris?

MR BING: Just at, like, a higher level for a moment, in terms of conducting the operations overseas, a lot of times when you're trying to target and adversary network in Afghanistan or somewhere in the Middle East, ultimately you are looking at computer networks that may be spread in other parts of the world, be it Germany or some other place.

One of the operations where this was discussed was Glowing Symphony, one of the few operations that was reported on the press in detail. The conversation was that it needed to target infrastructure in Germany, for example. What is the process like to have a conversation with the Germans or another country when those boxes are in an ally and, ultimately, to conduct an offensive operation, you need to touch those?

MR. LUBER: So I'll turn that to one of our operational commanders.

MAJOR GENERAL SELECT HAUGH: So I'll take it. I think, in general, what we have seen as both our authority has matured and as our force has matured, we are proud of the processes that we have in place to be able to work with our interagency teammates that allow us to make sure that we are all going the same direction and we're not –and we're using all of our resources to meet the outcomes that –I think from our –what our nation would expect.

In terms of international partnerships, we don't normally, as the tactical command, work those things. But there are structured processes through the executive branch that allows us to reach out to any partner in a clear way that allows us to communicate when it's appropriate for any type of action. And that goes beyond cyber in terms of how those processes work.

QUESTION: I wonder if you could talk a little bit more about the effort in the 2018 midterm elections. There has been public reporting about a couple different things that the Cyber Command/NSA did, Cyber Command, in particular. I know you feel it was successful. I wonder if you could talk a little bit more about what kinds of things, specific things, Cyber Command did to counter the disinformation campaign that came out of Russia.

MAJOR GENERAL SELECT HAUGH: So I think doing –for the things, the areas, that we're comfortable talking about, like, there is specific operations that, in terms of details, we defer that to OSD for discussion. But the areas that I think that are really clear that are at its foundation, kind of coming back to the same line of effort that I talked about, is the partnership between NSA and Cyber Command to gain insights into adversary activity and share that across the executive branch and then be able to pass that to stakeholders in the states and industry through our domestic partners, that, I think, we are really proud of.

That allows for both of our missions were successful in terms of NSA being able to produce intelligence in a very effective way and Cyber Command to be able to position itself to defend critical infrastructure fast. So that, I think, is, at its foundation, one of the things we're most proud of. Areas that we have talked about are the defensive missions because those defensive missions that we did overseas were clearly intended for us to be able to gain insights into how adversaries operate in areas that we believe that, in this case, one of the NDS competitors was operating in. And that allowed us to gain insights in a way that we hadn't in the past.

QUESTION: NDS?

MAJOR GENERAL SELECT HAUGH: National Defense Strategy.

QUESTION: All right.

MAJOR GENERAL SELECT HAUGH: So that our approach to that was different. That was something we had not done before. We had actually been constrained to only operating our forces on the DODN, on the Department of Defense Network, and so in the NDAA, giving us the authority to move off the DODN and then the Secretary of Defense authorizing us to do that. And we are proud of how it was done, meaning we worked really closely with the Department of State.

We worked very closely with European Command to be able to do those missions. And to the –and at the end of those missions, we had a more secure ally. We gained insights that we wouldn't have had otherwise, and we were able to share those in a very transparent way with industry directly through the VirusTotal initiative. So those are the areas, I think, that, really, we took a lot away from in a maturing command, our ability to quickly gain insights and then apply those and share them in a way that we are pretty proud of.

MR. LUBER: Does everybody know what DODN is? Yeah, it stands for –

MODERATOR: Martin?

QUESTION: General Glavy, JTF-Ares, just the ISIS problem so you get to deal with, to the best of your ability, can you characterize the level of engagement you are seeing right

now, and what sort of stats and data metrics you can provide in terms of Twitter accounts you have taken down or online forums you have taken down, members you are seeing online, that sort of thing now three to four years into JTF-Ares being around?

MAJOR GENERAL GLAVY: So certainly there is a degraded state writ large that we see. We're certainly working very closely with Central Command, Operation Inherent Resolve, and now Special Operations Command and the other COCOMs on this transregional piece. We don't underestimate the adversary, certainly, on any step we've known, that they have been able to maximize the use of the cyber domain to create their messages and disseminate them.

So, obviously, we want to do our very best to deny, disrupt, degrade their ability to do that, which we continue to do daily. So, overall, I would tell you we're in a degraded state but not a complacent state because we know it's a –it's an adversary that has the will. So we want to do everything we can to deny their ability to use it in the cyber domain.

MODERATOR: Todd?

QUESTION: Good morning, sirs. Cyber Command became a unified combatant command a year ago. Who is the biggest beneficiary of whatever it is, the things that Cyber Command is doing? What would be the repercussions if you all hadn't stood up?

MR. LUBER: Well, I'd say the continued maturity of the command. To be a full combatant command demonstrates not only that our cyber mission force is ready, that offense and defense are working collectively together, that the nation can partner with a more mature command, whether it's with DHS, with FBI and with other parts of the interagency. So I'd say the whole government benefits from Cyber Command being a full combatant command. In addition, I would have to point out that we have deepened our relationship with our allies. And we continue to engage in many of those different areas to improve those partnerships.

MAJOR GENERAL SELECT HAUGH: I'd add we just completed a very large exercise that went across multiple combatant commands. And one of the things that we've also watched over this year is the maturity of Cyber Command's ability to work with the other combatant commands. And our J3 and what General Moore likely described in some of that is our ability to do command and control of our own force and then be able to really integrate with the geographic combatant commands is an area that it's now matured. It's not a question. It's now –we can operate really closely with multiple combatant commands simultaneously in a space that –that Chris described, you know, that really spans beyond geographic boundaries. And I think we are –I think that's been a major step forward in our abilities.

QUESTION: General Glavy, on the JTFA mission, I just want to get some clarification on something you said earlier. Are you now also responsible for global counter-violent extremism efforts, and does that kind of help as you support SOCOM globally to kind of provide that connective tissue between the geographic combatant commands to kind of have a more holistic picture of those threats as they kind of transgress, you know, regional boundaries?

MAJOR GENERAL GLAVY: Exactly. And that's exactly my answer. So obviously, as General Nakasone transitioned the --

MR. LUBER: Question –

MAJOR GENERAL GLAVY: –command to MARFORCYBER, I have a relationship, a general support relationship, defined to Special Operations Command. And Special Operations Command also has the mission set of the global violent extremist organization mission. So it worked out very well that I continued to support Central Command in the inherent resolve mission, which we do, but also now taking on this more global transregional piece, working very closely with SOCOM, who also has to work very closely with the geographic combatant commands, which we do as well. But it does provide a great synergy having SOCOM and spent a lot of time with them and have a team down there planning with them intimately to make sure that we are ready as they execute their plan as well.

QUESTION: So does that mean that you are operating over all geographic commands and are you –I mean, are you basically working where SOF is working? And is it mainly messaging that you are trying to stifle?

MAJOR GENERAL GLAVY: So it's –you know, it is full-spectrum cyberspace operations. And the term that we have used to describe this is the cyber-coordinating authority for violent extremist organizations, which means that, you know, based on the scenario, based on the mission, obviously we work very closely with Army and Africa Command; right? We work very closely with Army in Central Command. But we are the cyber-coordinating authority that the commander comes to us as we tried to coordinate/synchronize any type of operations that we may do, that Ares itself may do, or that Army Cyber Command, Joint Force Quarters –Joint Force Headquarters Army may – may do as well. So it's this coordinating authority that we do in support of global VEO operations, again, you know, with the geographical combatant commanders but also with Special Operations Command.

QUESTION: And when did the authority –when was that given to you to have more of a wider aperture in pursuing these groups?

MAJOR GENERAL GLAVY: So it was given by U.S. Cyber Command from General Nakasone as a mission to my –to me as a component to him. And it was done in September as well as –

QUESTION: So when you took over?

MAJOR GENERAL GLAVY: Right.

MODERATOR: Shannon?

QUESTION: Right. Hi. Shannon Vavra from CyberScoop. So as –I think it was Mr. Luber. You were talking about, as we have more constant contact with adversaries and defending forward and persisting engagement, how does Cyber Command –and this is a question for each of you –think about the risk, then, that we have with more constant contact, that adversaries might then take up our tools and turn them around. And this obviously comes following the Symantec report that was issued yesterday. So I just want to get your perspective on how you think about that constant contact and getting closer to the adversary.

MR. LUBER: So, first off, there is always a risk calculus in any sort of operation that we take on in Cyber Command. And the commander looks at those risk scenarios every single day. When it comes to, you know, working in an environment where our tools will be used in our operations, we participate just like other parts of the U.S. government into that process, the vulnerability process.

And that is also a broader whole of government view of vulnerability equities and how they are looked at. So we are part of that process in U.S. Cyber Command, just like other parts of the Department of Defense. So, with that, if anybody else would like to comment –

GENERAL GINGRICH: No, I think we have –I would just say we have a very formal risk management –

MR. LUBER: Yeah.

GENERAL GINGRICH:–structure on every aspect of our mission set. Offensively, you know, what target are we going after? What tool are we using or series of tools? You know, how is the risk framed for that? Are we comfortable with that? Are we making the right decision at the appropriate level of our command. And then, every day as risk management on the defensive side with our censoring and our posture and our, you know, defensive scheme is constantly being adjusted. And, again, risk is managed by, you know, devolving those authorities down to the lowest level so we can be reactive in the cyberspace.

QUESTION: Just a quick follow-up. Does that, then, go to tracking, sort of, when we're releasing malware abroad, for example. Is there a way that we keep track of that?

GENERAL GINGRICH: I'm sorry. When we are releasing malware?

QUESTION: When we lace malware abroad, for instance, or we are going into adversaries' networks or intrusion.

GENERAL GINGRICH: So, yes. So that's what I was describing on the offensive mission management. A key component of that is risk management. And what does our –you know, our footprint in that context look like? What –you know, are we comfortable with the calculus there from a risk management, from a gain/loss perspective, etc.? It's very well-managed. It's a very formal process. And the decision is made at the appropriate level.

MODERATOR: Ellen?

QUESTION: Yeah, thank you. On –going back to lessons learned from the 2016 engagement and looking ahead to 2020, I wondered if you could expound on that a little more. Do you recall you described working with the –with partners or allies overseas and to understand where the adversary –take that with Russia –was operating, what they were doing? Are you continuing to do that with these same partners and with others? Is this campaign continuing today, and are you increasing the tempo now that we're, you know, in 2019, looking ahead to 2020? And I heard synthetic ideology mentioned. Is that the – is that sort of the umbrella term for this?

MAJOR GENERAL SELECT HAUGH: No, I'm just going to give you –

QUESTION: Okay.

MAJOR GENERAL SELECT HAUGH: –the big picture. So from a –

QUESTION: Yeah.

MAJOR GENERAL SELECT HAUGH: –from a 2018 to 2020 perspective. So 2018, we –the Secretary gave guidance to General Nakasone in and around the May time frame. When he took over, he said, "I want you to focus on this." So that meant we built a partnership between NSA and Cyber Command in how we approached 2018. So now, for 2020, we benefit from all that work.

QUESTION: Mm-hmm.

MAJOR GENERAL SELECT HAUGH: So the work that we went through, the lessons that we learned, the things that we said, this is now an approach we want to

continue, this is one that we didn't get as much value from, we're allowed, then –we can now focus based off of that. And what also starts, it is very different.

In 2018, in some cases, from Cyber Command's perspective, as a maturing force, we had to build new relationships, whether that was with DHS, whether that was with FBI or our teammates in the Department of State. All of those were –were now your –we had to build together in a really short time frame those close partnerships. We have now gained the benefit from that hard work in 2020 that we are starting from a set of foundational partnerships that have now –we have already worked together.

And they know what to expect from us but also know that we want to be a good partner with our interagency teammates and then with the other combatant commands because there are opportunities, as we look to do those missions overseas, where they are helping –it's helping build their partnerships. And they have teammates that they want to grow cyber-capacity in.

And, from our standpoint, we want to be able to understand what adversaries are doing. So there is an opportunity there for both the geographic combatant command and U.S. Cyber Command to both reach objectives but they are different objectives. So that's areas that we want to continue to grow. And we want to do that anywhere that there is going to be a potential adversary that would also target our electoral process.

QUESTION: Are you actively working now overseas with partners to try and discover and uncover potential tools that, you know, an NDS adversary might be using --

MAJOR GENERAL SELECT HAUGH: Yes.

QUESTION: –against us for 2020?

MAJOR GENERAL SELECT HAUGH: Yeah.

QUESTION: You are doing –so that work is ongoing today now. It's active

so --

MAJOR GENERAL SELECT HAUGH: It has not stopped.

QUESTION: It has not stopped. That is part of this whole persistent --

MR. LUBER: Persistent engagement.

QUESTION: Okay. Has it –has it increased at all in tempo?

MAJOR GENERAL SELECT HAUGH: I think what we're –we –what we are doing right now is we –we've –I would say, right now, it's been –it's been relatively constant. It will grow now that we have the authority. We're resourcing more of our defensive kits

that will be optimized to this mission. Those are areas for us we think are just really good partnership opportunities.

QUESTION: And as we get closer to the 2020 election itself, can we expect to see more –you know, other operations, the sort that might have engaged in, in 2018?

MAJOR GENERAL SELECT HAUGH: My expectation of that is really going to be driven by our adversaries. Our goal is to have no interference in our elections.

QUESTION: Mm-hmm.

MAJOR GENERAL SELECT HAUGH: We are going to support DHS and FBI in the missions they have been assigned. But, ideally, no foreign actor is going to target our electoral process. And then, from our standpoint, there are no actions that would be expected in the –

MODERATOR: Dustin, over to you.

QUESTION: Just to follow up on that line of questioning from Ellen, so, you know, you have talked a lot about persistent engagement and the value of understanding what the adversary is doing. So, you know, leading into 2020, if there is a situation where you observe an adversary making a targeted campaign against a presidential candidate, you would presumably, I guess, work with your partners, DHS/FBI to decide how to address that and, you know, including notification, potentially, to the candidates.

So, one, is that correct that that would have a process of work? And then, in that situation where an adversary was engaged in the targeted campaign against a candidate, would the –would the notification process also occur interagency to inform the White House of that campaign as well?

MAJOR GENERAL SELECT HAUGH: So I think that would largely fall outside of U.S. Cyber Command in terms of ODNI would largely handle anything from an intelligence perspective that would be discovered and communicated. But that –from a Cyber Command/military standpoint, probably unlikely that we'll be deep inside of that type of discussion.

QUESTION: Are there any situations where you feel that it would be involving candidate notification or, you know, indirectly, presumably, through the partners, DHS/FBI?

MAJOR GENERAL SELECT HAUGH: I think that would be unlikely from our standpoint.

QUESTION: I guess two quick ones. Under this NPSM authority, can you give us an idea for how many more operations have occurred if it has involved, like, the difference,

if it's provided –since it's provided more authority, can you give us a broad number for how many more have been conducted under this authority?

MAJOR GENERAL SELECT HAUGH: Probably drawing a distinction, is your question the change in the law under the NDAA?

MR. LUBER: Right.

QUESTION: Yeah. So under the previous authority with the PPD 20 –yeah, our understanding in the press is that this new authority allowed for these operations to be more easily approved. What I'm asking is what has been the difference in terms of the number of operations that have been run.

MAJOR GENERAL SELECT HAUGH: Yeah. I think, from our perspective, we wouldn't be comfortable providing any sort of scope or scale on either, either under PPD 21 –13.

QUESTION: Okay. This –this DreamPort organization. My understanding is that this was at least partially founded by a guy named Karl Gumtow who –whose organization, CyberPoint, was previously involved in standing up cyber operations in the UAE. Has that been a concern at all from your standpoint?

GENERAL GINGRICH: I'm not going to be able to comment on Mr. Gumtow's previous organizations. What I can tell you is the engagement that we have with DreamPort has been a very positive engagement, whether it's through the partnerships that we've had with industry coming into that particular unclassified area, the outcomes of our rapid prototyping events, or even the future opportunities that we have to engage with academia and industry together. I'm very happy with the progress we're making in that particular area.

MODERATOR: Julian?

QUESTION: What is the current cyber threat from the sort of –from Russia, China and Iran, and what part of Cyber Command handles Iran? Is it –is it part of Task Force-Ares with the sort of extremist groups Iran supports, or is it another entity within Cyber Command that would do defense and, if necessary, offensive operations against these three adversaries?

MAJOR GENERAL SELECT HAUGH: You want to start?

MAJOR GENERAL GLAVY: So I can start. So just –so Ares, obviously, focused on the violent extremist organizations. So Joint Force Headquarters Army primarily is the –provides general support to U.S. Central Command. And so they would be the ones primarily focused on Iran, the country of Iran. And, additionally, General HAUGH and his team, as well, has a mission in Iran that he may want to touch on.

MAJOR GENERAL SELECT HAUGH: So our focus would be if it's a malicious cyber actor. And so that's one of the –that's how we've organized. And so that –we do that work from the defend-the-nation/defend-critical-infrastructure perspective. But also do it in close partnership with Joint Force Headquarters DoDIN, which runs the Department of Defense network for General Nakasone. So they're responsible for the defense of the DoDIN, so they're thinking about threat all day long, as in terms of anybody that would threaten the Department of Defense and any associated network, and then we're in support of them if it's targeting the Department of Defense.

QUESTION: And in terms of the broader question of what is the level of threat from these three adversaries, China, Russia, Iran, right now in terms of compared to recent history, is this higher than recent times? Is it lower because we're not in an election cycle right this instant? Is it higher because we are sending an aircraft carrier toward Iran right now very publicly? What is the current –

MAJOR GENERAL SELECT HAUGH: Do you want to take the beginning and I'll --

MR LUBER: I don't think we can get into any details of the level of current threat right now. But what I'll tell you, as a command, we have to be prepared for all threats, whether it's our defensive teams protecting the Department of Defense networks, working with our partners in DHS and FBI in critical infrastructure or it's our efforts to operate in other areas of the world.

So I am not going to say that any particular threat is higher or lower today because cyberspace is in constant change. Twenty-four by seven, we are engaging. Twenty-four by seven, you know, we see adjustments that we need to be able to be ready for at any given time.

Tim.

MAJOR GENERAL SELECT HAUGH: And I think where you would –if you look at what General Nakasone testified to, and why we are at a persistent engagement strategy is, adversaries are conducting intellectual property threat. We've had adversaries target our electoral process. That is, they're running constant campaigns. And what we're working on is, what's the role of the Department with our teammates in DHS and FBI to counter those campaigns?

QUESTION: On the CMF, General Nakasone testified earlier this year that he predicted that at one point it's going to have to grow beyond the 6,200 that are currently operating. Do you share that assessment and is there any sort of planning going on for that day? Are you looking at anything like do you have a number in mind in terms of on that issue? And then quickly on the J2 (ph) areas, I understand there is talk about moving your authorities underneath this new NSPM 13. Is that done or is that still ongoing? So however you want to go.

MAJOR GENERAL GINGRICH: So I'll start off. No, there is no number that we are shooting for. So again, just to put it all into context, so we've achieved FOC just about a year ago, I think it was in June of last year when our final –the 133 teams became FOC. What General Nakasone is really working on and focused on right now is defining readiness from a personnel perspective, from an equipment perspective, from a training perspective. And ensuring that we have those feeder pipelines of equipment, acquisition and procurement of everything from recruiting through the training and fielding of cohesive cyber mission force teams, whether defensive or mission teams or support teams, really focus on trying to define that, getting a good measure of his force. And then it's going to be based on operational experience and operational realities. And we will start to –you know, we are trying to collect the data that would inform decisions like that.

But I think we are very early in that process to determine that we have to grow and we have to grow by X amount. But we're looking at it. But our real focus right now is on readiness and how do we define that.

MAJOR GENERAL GLAVY: And unfortunately, I can't really discuss any of the specifics of NSPM 13. We do follow processes very, very closely and diligently. But any specifics, not appropriate.

QUESTION: But you guys were founded before that was created, so it seems like there's two lanes. But I understand there's talk of putting it all in the same lane, same processes. Can't go there?

MAJOR GENERAL GLAVY: Yeah, sorry.

QUESTION: Okay.

QUESTION: (Inaudible) a hundred Cybercommand service members operating at the lowest levels of DoD operations, how are you benefitting the soldier on the ground or the sailor at sea or the airman in the air?

MAJOR GENERAL GLAVY: I'll take a first shot at that. So I also have, part of my command, I run the Marine Corps Enterprise Network. So this is part of the DoD information network that supports the Marine Corps and the Commandant and all the Marine Air Ground Task Force missions. So we take that job very serious.

We focused again, very –in a very compliant state, very disciplined state, ensuring that our Marines are doing the right thing on that network. We treat the network very much like a weapons system, ensure that it's respected and taken care of and we operate it accordingly. Because it's very important to how we are going to fight. And I think that's the best –you know, the Marines kind of support us –really, support us in that mission, but it's obviously in our best interest as a warfighting entity to ensure that that network is run and run well. And vast majority of the time, you know, it's not my Marines on that

network, it's those Marines at the forward edge that are actually interacting. So it is really important that we take great care of the network. And those Marines forward are part of that.

QUESTION: General Gingrich, I was hoping you might be able to expand a little bit on the JCWA. You know, obviously, there's, you know, CYBERCOM has some unique authorities in terms of acquisition. But they are still executive agents for training and, you know, cyber internal platforms. But from a tool development perspective, I mean, how are you looking to kind of ensure that, you know, service-specific tools aren't developed anymore, that it's kind of, you know, something that can be used by everyone, everywhere?

GENERAL GINGRICH: And you just described the goodness of the JCWA, because it helps us have that dialogue. It helps us understand and brings clarity to investments within each of these spaces and it's helping us divide up tools. For instance, who is procuring what tools? We don't have enough acquisition authority to meet the needs of the entire cyber mission force. So what you've talked about are some constructs that the Department has used, like executive agent. Where, really, what the JCWA is, it allows us to communicate directly to a service, whether it's the Marines that are going to procure a specific capability. Through the requirements process, we can govern sort of what they are buying. We can advocate for them so that they have the resources that are there. But through that construct, we don't need an executive agent relationship where one service buys tools for everybody.

Now we are starting to, in doing it in that construct, now we are using the full power and capacity of all of our services as well to procure cyber capabilities. So just think about that. You know, $75 million here internal to U.S. Cyber Command is not enough. Now if we can leverage the Army, Navy, Air Force and Marines to make specific investments and make sure that they are deconflicted, so that we are effective and efficient in use, that's what one of the benefits of the JCWA is. And I think we won't see the need for executive agent type relationships, like the Army is the executive agent for persistent cyber training environment.

I think we can use other means, existing authorities, rules and regulations within DoD to become even more sort of agile in this space.

QUESTION: How does that work on an ongoing basis? Obviously, things change so quickly in cyberspace. I mean, is it, you know, you're going to the services to nominate them? Are they nominating their capabilities? It's obviously, you know, dependent on their own, you know, rapid –potentially rapid acquisition authorities?

GENERAL GINGRICH: Yeah, absolutely. So I am kind of the broader strategic here at Cyber Command, trying to work with the Department of Defense and the services to

work on the next program objective memorandum, POM 21 to 25. Meanwhile, trying to justify the President's budget request for FY '20.

Now, as you work closer back and you work down into the service cyber components, they have capability developers as well as their own supporting infrastructure through program managers, et cetera, other organizations that can help them in the short term, quick term type events. So what you are seeing is a maturity across this entire space.

I would say in the past, we were very good close in, doing the right now, I have a team on net, is using a tool that needs to be modified. So we pull it back in, we do the modifications, we give it back to the team and they're on there. And we've always been very good at that. What you're seeing with the JCWA and the maturity of the command is how are we projecting these out into the future so that we can start to do this really at industrial level, industrial scale. That's where that's driving us.

MR. LUBER: Yeah, I would just add, it's an enterprise approach. So just like any corporate enterprise would look at how they would manage a broad business, we are looking at Cyber Command as an enterprise. And the Joint Force Headquarters is part of that enterprise. So as a command, by having this set of standards and opportunities, we bring together the best of all the different developers, the best in breed of all the different tool capabilities. And, most important, the talent of the people. That is one of our most cherished resources that we have in the command and across Cyber Command is the –is the people. And having capabilities and systems where people can collaborate across with each other allows us to be very effective, both in our missions to defend and to present actions when necessary.

QUESTION: General Haugh, as you're looking at the analysis, as you're doing analysis on the 2018 elections, it sounds like you are very happy about how you responded. But, of course, you know, you had lessons learned, I imagined. So what are some of those things that you're learning about? What are some of the elements of the plan that you're looking to tweak? And are you content with your ability to respond in a short time line? And are you looking for additional authorities going forward in 2020?

MAJOR GENERAL HAUGH: So I think the area that we collectively want to just keep getting better on every day is speed. Being able to move quickly in terms of anything that we're conducting from a Cyber Command perspective to be able to rapidly process, rapidly share, enable and then use that within our own planning. And we're –we felt like we did a good job. But that's a space in cyber that you can always be putting energy towards, just increasing speed across all of the activities that we'll conduct.

The other areas I think that –is how do we continue to balance our collective resources when we look across, to make sure that we don't have overlap anywhere. And if it is, if there is some overlap, it's conscious. We did a good job of that but that's an area that we will want to communicate with each of our partners. And we've already started that

work, to make sure that we're all looking at this and understanding who needs to be communicated together across our interagency so that we're all moving in the same direction.

And then I think, from an authority standpoint, we're at a spot that right now what we really want to be focused on is the partnerships on the interagency side. Any discussion of authorities from our standpoint right now is premature.

QUESTION: What do you mean, focus on the partnerships?

MAJOR GENERAL HAUGH: It's about the connective tissue. So for us, and this is absolutely literal to General Nakasone's strategy, if –the lead for the federal government in critical infrastructure protection is DHS. So that partnership, as CISA forms in its role, with Chris Krebs (ph) and their work that they're setting out now to look at the national critical functions, we've got to make sure that we're connected at all the right spots at DHS to enable their success. And so that is –when we look at the elections, that's number one, supporting DHS in its role there.

And then number two is FBI, as they've worked –they've done an exceptional job of organizing from an influence perspective. And so certainly, if there's anything that we learn, we want to make sure it gets to the exact right spot so that they can be the most effective with it. And that's an everyday thing as we continue to go forward.

QUESTION: One quick follow-up to that, just moving forward to 2020, David Hogue of the NSA recently said one of the gaps he sees the NSA has is managing misinformation and that kind of warfare on social media platforms. Do you see Cyber Command as having any role to play in misinformation warfare and combatting that? And then I can also tack on, how do you look at measuring NSPM 13's success? How, I think you said at a recent event, I think it was at the (inaudible), that you're measuring success based on whether you can work with DHS and State if they are issuing demarches and things like that. What about the policy outcome? Are you seeing any decrease in attacks from adversaries or an increase? And are you measuring that right now?

MAJOR GENERAL HAUGH: I think from our standpoint, assessment is something we're working on all the time. That's across the whole department. Is, as we apply resources to a problem, as we achieving the outcomes we intended to achieve? That is a constant level of work that we're doing with our partners.

What was the first part of your question again?

QUESTION: The first part of the question was misinformation.

SENIOR OFFICIAL: Misinformation and Dave Hogue.

QUESTION: On social media platforms.

MAJOR GENERAL HAUGH: I think this is an area when we start to think about roles and responsibilities. I think from our standpoint, we're looking outside our –outside our borders. That's our focus. When General Nakasone and the Department talk about defend forward, we're really looking outside our borders. That type of information is probably best left, from a real focus, from a domestic agency standpoint as we go forward. But it's an area where we want to contribute our understanding based off of what we do in our defend forward operations, but not really in the social media space.

QUESTION: Okay, thank you.

QUESTION: Yeah, and just following up on that, and a question I think I asked earlier, when you said you are actually actively now working in partners' networks overseas, I mean, I take it that includes the U.K., Macedonia and –what was the third one that someone mentioned earlier –the same three? And you've expanded beyond that?

MAJOR GENERAL HAUGH: We have redeployed out of some of those.

QUESTION: Okay.

MAJOR GENERAL HAUGH: We've got some that are in different stages of work between the geographic combatant commands, the Department of State and those individual nations. So we don't –we are really going to be driven in some cases by the adversary.

QUESTION: Does that defensive work extend to actually, for instance, preemptively, you know, taking out an adversary's platform to help the partner, to defend your partner?

MAJOR GENERAL HAUGH: Let me first kind of frame where we fit, like so in these defensive operations.

QUESTION: Yeah.

MAJOR GENERAL HAUGH: So in the defensive operations, there are things that are going on every day with the geographic combatant commands that are outside of U.S. Cyber Command. So they are out doing partnership activities with their own cyber forces to help them secure networks.

What we are trying to bring in our defensive operations with them is really a focus on the adversary. And also it enables us to be able to do our defend forward missions. So those we view as partnerships going forward.

I think in terms of the other question, that's probably getting into a level of specificity I am not real comfortable –

QUESTION: Okay. And then I just wanted to pivot for a minute to China. And how would you describe –what does persistent engagement against China look like? Since the threat from China in cyberspace is one that has, you know, largely today been, you know, in the realm of economic espionage, industrial espionage. So how does your persistent engagement activity look like against China?

MAJOR GENERAL SELECT HAUGH: I think one is from the outset, is it's not just cyber solutions to China's cyber activity. It's how we as a nation and then through with our allies set what are the expectations of international norms and how –what that looks like. And then how do we, as the Department of Defense and our resources, inform all the executive branch responses? That's where we –we're going to be a player in that discussion. But in reality, this is whole of government, whole of nation.

QUESTION: So it's more intelligence gathering to inform the policy makers who might want to devise other options?

MAJOR GENERAL SELECT HAUGH: Comes back to exactly where General Nakasone is. It's two thirds enabled and then be prepared to act if called upon. But it's really in this case, how do we inform and partner with all those same entities that are working this, whether it be DHS, FBI, State, and inform what is the best approach if there is any nation that's out there acting outside of international norms in things like intellectual property theft.

MAJOR GENERAL GLAVY: Persistent engagement also has a defensive side to it and General Nakasone talks a lot about this. So I have a lot of forces in INDOPACOM, Marine Corps forces that we have very much a persistent engagement from a defensive standpoint. What I mean by that is defensive cyberspace operations, the ability to maneuver on our own networks, right? We've got to be looking for the adversary diligently, constantly. So this is not only about –you know, about offensive cyber effects operation but it's also a defensive cyber piece that he talks extensively about, that we've got to make our own luck, we've got to be good in our own networks and our own capability, find the adversary and eliminating them.

MR. LUBER: And as I spoke earlier about our work that's going on over at DreamPort, we're looking at zero trust because we want to make it more difficult for adversaries to get into our Department of Defense networks. We're not just looking at it because it's a cool buzzword. We're actually focusing on how do we make sure that the right people are accessing the network at the right time from the right location and that others who are trying to come into those networks are denied access through some of the zero trust principles that we're looking at right now.

So it's not just the persistent engagement. Very important. But also that persistent innovation. How do we harden that attack surface? How do we make sure that what we

learn in the Department then gets shared with broader sets of our government and broader sets of our critical infrastructure so we make it more difficult for an adversary?

So that's why when I said that NSA was one of our most important partners, is that deep technical expertise from NSA, working with U.S. Cyber Command, working with the industry, to help us ensure that we are setting the conditions for the future on how we will operate in cyberspace, protect and defend in cyberspace, and make sure that those adversaries who are trying to take advantage of the United States or our allies are meeting difficult times in getting access to our critical information.

MODERATOR: And so just an overview, we have about 10 minutes left. These gentlemen have a hard stop to the next thing. So --

QUESTION: General Haugh mentioned working with CISA over at DHS (inaudible) recently announced national critical functions set. Has that list in any way –how does that list, you know, sort of guide your work in any way? Does having a list in any way sort of clarify or contextualize your mission?

MAJOR GENERAL SELECT HAUGH: So I think it does. Because when you look at the agreement between the two Secretaries was really about how do we work together. So of course we want to work together on the highest priority problems that allow for DHS's success but also is complementary to the work that we are going to do within the Department to make sure that we can meet any expectation. So we think they're taking a really good, logical step and approach and we are happy to partner with them and work those priority problems together.

QUESTION: And you mentioned the agreement previously, too, that was hammered out by Secretary Nielsen and Secretary Mattis –now acting secretaries on either side. Is that in any way a concern or impacted in any way by the change in leadership?

MAJOR GENERAL SELECT HAUGH: No, the agreement was really an acknowledgement of what we were working together. So it's really just –that was really to ensure that we had both departments aligned. But we had already been working it and now it was just –now, we've been executing it.

QUESTION: Two questions. The first one being, all these different government agencies obviously would like to speak with, for example, critical infrastructure providers for threat data as well as the financial sector. What do you think Cyber Command brings to the equation that makes it a good deal for these companies to provide data and to work together with you?

MAJOR GENERAL SELECT HAUGH: I think from our standpoint, it's complementary. And this is where the partnership with DHS and Treasury has been really important. If we look at once the secretaries signed the agreement, we don't

necessarily bring the expertise in what's critical within the financial sector, right? We're looking for Treasury and DHS to help us gain an understanding of what that is, so that as we look overseas, that we're now focused on the things that are important to that sector in a way that we wouldn't have done without the partnership with DHS, Treasury and the sector. And that's where some of these Pathfinder activities have been really helpful for us to understand what is actually critical and then how would we approach our operations from a different perspective to help inform their defense.

QUESTION: Can you dive more into like what Pathfinder is? We keep going back to that word, but I'm not sure if anyone here has a great understanding for what that is.

MAJOR GENERAL SELECT HAUGH: It's really just a pilot activity.

QUESTION: It's a pilot? Okay.

MAJOR GENERAL SELECT HAUGH: So it's our first attempts to be able to work through a more structured process that allows our defend forward to be complementary with the core mission of DHS and the sector specifically.

QUESTION: And the second question which is different is, was increasing investment in these cutting and innovative tools and techniques for offense, has there been increased investment or a different type of strategy in the protection of these methods and tools from the agency perspective? And when I say protection –

MAJOR GENERAL SELECT HAUGH: Diversity, you mean, more so than protection?

QUESTION: I'm talking about like efforts to make it so these tools are not used by an adversary or not leaked or in some way acquired by an adversary group.

SENIOR OFFICIAL: So safeguarding them is, you know, priority for us. And they are safeguarded. But then, you know, they're used in, you know, the cyber environment. And once they're out there, they're out there.

You know, we take –we have learned from NSA, you know, that's one of the benefits of the partnership is we have learned from them on TTPs, on tool development, et cetera. So we are trying to internalize and capture, you know, sort of best practices with that. But at the end of the day, once you have used the tool, it's out there. It is. And I'll just leave it at that.

QUESTION: It gets back to that risk assessment you were talking about, correct?

SENIOR OFFICIAL: It is part of the risk assessment.

QUESTION: In the context of the Russia small group, I think at some point in this data, there was talking about a little bit –sometimes there is a tension between an operation and intelligence collection. And that's, in some ways, the tension between Cyber Command and NSA. And I am wondering, obviously you can't talk specifics. But in general, how were –was that an issue when you're talking about the midterm elections? Will it be an issue going forward, of how do you make the case of, well, we need to still collect on these adversaries, versus we need to do something to deter or stop it? And how does the sort of integration of Cyber Command and NSA sort of help with that sort of cost/benefit analysis?

SENIOR OFFICIAL: Do you want to take that? Just kidding.

(Laughter.)

MR. LUBER: I think for us, this was an approach. What General Nakasone drove towards was unity of effort. And so starting from the outset as a team with complementary missions, it allowed us to avoid those difficult discussions as we move forward through this process. And we think we were really successful in how we made sure that the National Security Agency could meet its critical role to inform while we were preparing, informing and also generating options as required by our leadership within the Department. And then the maturity within the Department of how we coordinate all of our activities, really from our standpoint went really well for every activity that we did, both informing and then preparing.

QUESTION: Lightning round. So I (inaudible) at the top about acquisition authority of 75 million. Several months ago, General Nakasone testified that you'd only spent 45 million and 60 to 65 would be spent before the end of the fiscal year. You're saying now you will hit the 75 mark? And if that is the case, did something happen between now and then that –or were you just afraid that you have to spend it or you're going to lose it?

GENERAL GLAVY: Well, I'm optimistic. We'll put it at that. No. So we could potentially –so acquisition is a dynamic environment. Are you ready to go? Do your solicitations meet the time line? You know, do the respondents meet the time line? So, you know, it's hard to say whether we would actually get to 75 million.

What we are anticipating, as we mature –because part of this is getting back to our workforce. Do we have the acquisition workforce that we need? And the fact is, we are still growing that acquisition workforce. And that is one of the limiting factors to executing our $75 million. So we are doing everything that we can to bring on additional talent so that we can meet that 75 million. We just don't want to run into a situation where we're in a June, July time frame and we've already exhausted our $75 million acquisition authority for that year, now what do we do?

And so that's why, when I said negotiation, it's really discussions with Department of Defense, Congress and us to make sure that we have the appropriate level, where we don't over-ask but that it's balanced, based on our maturity and our ability to execute. Because we see the value of it. It really enhances the timeliness of what we can acquire.

QUESTION: To follow up on Julian's question about the NSA, Russia, Cyber Command small group, is it General Nakasone who is chairing it and you meet day to day? I'm just curious about the leadership structure that allows it to be so seamless. Is General Nakasone driving the car? Are you? Who is?

SENIOR OFFICIAL: So the way that General Nakasone structured it, he's the leader of both organizations. He wanted to ensure that there is unity of effort so he put NSA and Cyber Command together to co-lead the Russia small group. So that day-to-day management of those activities was done as a co-led activity between NSA and Cyber Command under his guidance to both organizations.

SENIOR OFFICIAL: At the same time, right? So you get the guidance at the same time. He gives direction. He gave us the orders to move forward to work as a team.

QUESTION: But I'm curious. He's a busy guy. Does he give the guidance to you or is it to another general here in the building or how does it –

SENIOR OFFICIAL: So he had a co-lead from U.S. Cyber Command and a co-lead from the National Security Agency that every day sat down together to be able to execute the tasks that he was giving to both organizations. And this was –and this was where it's unique. Him being the leader of both organizations, he was able to create that battle rhythm of coordination to ensure that NSA could meet its mission and Cyber Command could meet its expectations in a complementary way.

MODERATOR: Martin, you had the honor of the last question. We've reached the time. So I thank you all. We've got to get these guys to their –

PARTICIPANT: Thank you, everyone. It was great speaking with you today.

###