Inaugural South Carolina Cyber Consortium Luncheon
Air Force Secretary Deborah Lee James
6 May 2016

SECRETARY JAMES: [in progress] very kind introduction. I always appreciate when it's pointed out that I've had more than 30 years of service, because I started when I was nine, in case there's any math majors in the audience. I also want to thank the South Carolina Cyber Consortium at large for hosting this luncheon and congratulations, by the way, on establishing this important effort. And it is certainly my honor to be kind of the inaugural keynote speaker, if you will, on what I'm sure will be one of many, many more occasions. And by the way, if I may say, it is always just a personal treat for me to be able to return to Charleston. And I look around the room, I see old friends and colleagues. I see some new faces as well.

And it may be that not everybody realizes, so I want to tell you that I actually lived and worked here in Charleston during part of that SAIC career from 2007 to 2010. So this feels like coming home to me. SPAWAR of Charleston was my top customer in those days when I was the General Manager for the SAIC unit and I see, of course, Dave Monahan and Bob Miller here in the audience. I also served during this period on the Advisory Board of the School of Languages, Cultures, and World Affairs at the College of Charleston. And, indeed, later today, I get to return to the College of Charleston to give the commencement address for the class of 2016. And two years ago, I did a very similar effort -- I see Keith Plemmons in the audience. I was on the Advisory Board at the Citadel, School of Engineering, and I got to deliver the commencement address two years ago at the Citadel and how cool and what an honor that was for me.

So for all of you who didn't know that, I'm putting out I got some serious street cred here

in Charleston, you all. So it's wonderful -- wonderful to be back and, of course, fantastic to be back to the Trident Technical College as well, which, as has already been noted, the premier hub for delivering cyber security education to the workforce of South Carolina. And I certainly want to thank you in particular for partnering with SPAWAR on an initiative that's already been mentioned, but I want to give it a shout out. And that's the Palmetto Cyber Defense Competition. In my opinion, we need more events -- not fewer, but more -- like this so that we can collectively inspire more of our young people to prepare for cyber careers and for stem careers I'll say, generally. We need more young people like this in both government and industry.

Well, with that as an intro, let me just say, ladies and gentlemen, I am Secretary of the Air Force. So I wouldn't be doing my job if I didn't give you a brief report on the state of your and my Air Force. And as we sit here today and enjoy comradery and a nice lunch together, I want you to know that your Air Force is doing a fantastic job around the country, around the world and it is the busiest Air Force that we have ever been certainly in the 30 plus years that I have been personally an observer on the scene of our national defense -- both in government and in the private sector.

We have five core missions in our Air Force. They are air and space superiority -- and I want to also call out Colonel Gentile of the 169th Fighter Wing, McEntire, the Air National Guard, because you are squarely in the fight of air and space superiority. That's one mission. We also do intelligence, surveillance, and reconnaissance, global strike, command and control, and rapid global mobility. And a shout out to the 437th and the 315th Airlift Wings at Joint Base Charleston, because they are squarely in the mission of rapid global mobility.

These five areas, let me tell you, are in demand all around the country and all around the

world all the time. Moreover, the reason for that is because it seems like to me anyway, in the last two and a half years, which, by the way, happens to be how long I have been Secretary of the Air Force. But it seems like the whole world has changed in a mere two and a half years. For example, two and a half years ago, who ever heard of these people in the Middle East called Isil or Isis or Daesh? We never heard of such a group two and a half years ago. And yet right now, today, we -- the United States Air Force, as part of the joint force and as part of a coalition of more than 60 countries -- we are fighting these people and we are taking it -- taking it to them in a stepped-up, increased pressure way of late.

In the past year, our coalition forces have upped the pressure against Isil in the Middle East. We have flown more than 55,000 sorties in support of Operation Inherent Resolve. And, of course, the mission is is to degrade and to ultimately destroy these people who are trying to destroy our friends and our allies and also kill us in the Middle East and elsewhere in the world.

And if that's not enough, Russia invaded the Crimea and increasingly is flexing its muscles around the world. If you go back three years ago, if you remember, we were still trying to partner with Russia. All of that changed with the invasion of the Crimea. And, of course, Russia has also announced that they are modernizing their nuclear forces and they have already significantly modernized their conventional space and cyber forces.

And if that's not enough, we have a very assertive China who is now claiming nearly all of the South China Sea. And in order to bolster those claims of territory, they are building artificial islands basically on top of coral reefs in order to, as I said, bolster those claims. And, oh, by the way, China has modernized its conventional and nuclear capabilities as well as their space and cyber assets.

And then, of course, there's Iran. Now, although we and a number of other international

partners recently signed a nuclear deal with Iran -- which was good news -- it nonetheless remains a fact that Iran is aggressively acting and at times seeking to destabilize some of its neighbors in the Middle East. So, obviously, that's a huge concern to the U.S. and our allies in the region.

And, finally -- finally -- we've observed a complete whack job in North Korea, who has been conducting nuclear tests, rocket launches which could help them create the technology to be able to one day have an [ICBF] that could deliver very explosive kinetic effects to even the U.S. shores possibly. And all of this has been in defiance of U.N. resolutions. The people in North Korea are starving, but they are still spending heavily on their military.

So here's the bottom line to all of that -- all of this. The Air Force is playing a key role in each of these areas in a very complex and dangerous world. We're responding. We're reassuring. We're determined. We're working as part of our joint military force. We're fully engaged in every region in every mission area and we're doing so across the full spectrum of military operations.

And here's another bottom line for you. Every single one of the Air Force's missions that I described to you earlier depends on information dominance. Every single one. So our airmen at every level [inaudible] and accurate information to make key decisions and to remain agile in all of our domains. And when I say our domains, I'm talking about in the air and in space and in cyber space.

Now because our military's fighting edge is being challenged in ways that we've really not seen before, we can't take for granted our military and technological superiority. Because if we do so, we could well regret it and we could be putting American lives at risk. So with all of this in mind and knowing the importance of information dominance, the very first trip out of

Washington I took earlier this year was to San Antonio, which, for the Air Force, is where we have our 25th and 24th Air Forces based. And that -- those two units are basically the core of our cyber force. And, of course, wherever I go, it is always a huge pleasure to be able to visit with our airmen and San Antonio, certainly, was no exception to that rule.

Now, why was cyber at the top of my list? Well, because cyber space is a contested domain and it's critical. It's critical that we make ongoing investments today as well as in the future to ensure [inaudible] success. So today, with the remainder of my time, what I was hoping to do was to share with you some of my thoughts on our cyber space challenges and also then layout some of our efforts that we're undertaking to address these challenges. And as you'll see, the efforts basically include investments in people, technology, and also in key partnerships.

So observation number one. We need to shift resources over time from enterprise systems to war-fighting systems. So what do I mean by that? Well, let me [inaudible] a few statistics. Today the Air Force is spending roughly $4 million on cyber. But the truth in advertising, the vast majority of those funds go toward operating the network. Meaning we need to keep thing running and we need to fix things on the network when they break down. Now, regrettably, the bulk of our budget is not spent defending the network, which, of course, means that we need to assure our core missions are safe from cyber attacks, and also the bulk of the money is not spent on developing the types of offensive strategies that we need for the future.

The same, by the way, holds true for our people. We have about 67,000 people who are working in and through the cyber domain. The overwhelming majority of cyber space intelligence in acquisition work force professionals, however, are focused on operating the network. A relatively small number -- about 2,400 out of 67,000 -- are focused on defense and offense. So the challenge for me -- and really for others -- is how we over time shift money and

people away from operating the network and more of this toward defense and offense.

Now, obviously, we can't just drop the operations of the network because that's very important, too. But we need to shift our focus over time, and I believe that leveraging the private sector in different types of ways and increased ways will lead us in that direction.

So what are we doing about this? Well, as a starter, we've allocated about $670 million in FY17 to advance the defensive and offensive initiatives. Moreover, a key part of that, I'll say, our budget fully funds 39 what we call defensive and offensive cyber mission force teams and these units are the active -- the National Guard and the reserve component and they are designed to help us maintain cyber space superiority. Now 26 of those 39 teams are already at initial operating capability and we're going to be continuing to work on this over the next couple of years to bring them all up to full operating capability. So it's a good start, but, of course, it's not enough. We have to continue on the focus.

And so to that vein, we also started an effort last year that we call Taskforce Cyber Secure. This approach is designed to give a holistic view and to examine cyber security across the Air Force core missions and basically looking at what are our vulnerabilities, where do we need to focus our efforts, where are the holes that we need to plug. And this task force is going to be coming back and making organizational recommendations as well as resource recommendation where we need to put our money to get the biggest bang for the buck. And, by the way, I'm speaking not only in business and industrial control systems what we need to watch on those vulnerabilities, but also our weapon systems. We have to be mindful of possible vulnerabilities in weapon systems.

All right. So all of that is observation number one. That brings me down to observation number two. And that is that in my opinion, we in the Air Force are not doing an adequate job

today of training our cyber personnel in what I'm going to phrase -- what I'm going to call strategic thinking. All right, so, what I mean by this is is -- as I was telling you before, today we devote most of our talent and money to operating the network. Tomorrow the emphasis needs to be on functioning and fighting as cyber warriors. We've got to get our heads around that this could be, well, a war fight in the future. And we have train and we have to think appropriately.

Now to be fair, we are doing some of this today, but my point really is is that we are not really investing and training in sufficient critical thinking in cyber strategy -- that type of warfare strategy -- at least not in my opinion. So we're taking some actions to change this as well. First, we set up a Cyber College at our Air University at Maxwell Air Force Base last year and this Cyber College is specifically focusing on strategy. It's also a collaborative environment where our students can learn from leading cyber space strategists and leverage cyber technology moving away from traditional classroom settings where students, of course, listen to lectures and take tests and examinations.

Secondly, we [inaudible] cyber space [inaudible], which we placed at our Air Force Academy to help our cadets develop similar strategic thinking skills. And this is going to provide a centralized environment where airmen can work hand-in-hand with industry, academia, and agency partners to push the envelope -- the leading edge of technology.

And then the third thing I'll tell you about is that we released an Air Force Information Dominance Flight Plan recently. And this plan is designed to provide a strategic framework to articulate Air Force cyber challenges and how we move forward to meet our core mission. So it's designed to give our people strategic thinking and get our heads around the fact that cyber is a domain where we need to prepare to fight.

My third observation is we need to recruit at all levels into our force and we also have to

be open to create new approaches to attract certain types of cyber professionals, especially high-end programmers and kind of high-end thinkers.

Now back to the 24th and 25th Air Force. When I visited earlier this year, certainly I was briefed and I believe that we are doing a great job of bringing in the front door some fantastic young people and then we train them up to be part of our cyber force. But here's the hitch. As people become experts and really become much more senior in the cyber world, some of you in private industry can easily attract them away and there is no bonus in the world that we could ever offer to keep some of those high-end people if indeed money is the key thing.

So, of course, for us, hopefully, money is not the key thing. For us, money is an important thing, but it's not the only thing. We also offer interesting challenges. Challenges that are of a national security -- hugely important challenges, which if solved, could really advance the ball for our country and for the national security. So that's what we have to offer, but we have to be mindful -- be open to new ways of thinking about attracting and retaining people.

So here's a couple of examples of some new things that are going on. Last year, the Secretary of Defense announced an initiative called Force of the Future. And he's now rolling out pieces of this new program over time. And the basic principle, of course, the future -- is that, like I said, we in the military have to be a little bit more open minded, a little bit willing to try new things when it comes to bringing in people and then greater flexibility particularly as we try to retain those people when they become senior.

So we need to think about how to retain the experts that we have, as well as how to tap into the senior programmers and talent out there who may want to work on what is to them both very cool, perhaps short term project in the military, but for us could be crucial for solving a national security problem.

So how to bridge that gap? Well, there's no single answer and I for sure don't have all the answers, but once again, we're trying some new things. So last November, DOD launched what they called the Defense Digital Service. And here's how this works. Individuals from leading private sector tech companies are attracted or asked, if you will -- encouraged -- to take a leave of absence from those jobs. And then they come to work for us in the Department of Defense on a temporary basis and usually for a finite period of time -- perhaps a couple of years.

And so then, we might get a handful of technical experts -- three to five technical experts. They'll come on a project basis to the Air Force or to one of the other military services to address a specific problem that we're encountering perhaps in software development and delivery. And when they're finished, they'll go back to their civilian job. So this is something new that we're trying and what this does is it brings us, on a short term basis, people that we otherwise perhaps would not have access to and it brings us some additional diversity of thought in problem solving.

Here's another one. Last month, the Secretary of Defense launched a program he called Hack the Pentagon. And this initiative is going to be one in which we invite vetted hackers to test the Department's cyber security under a unique pilot program. And the idea, of course, is to conduct testing and find vulnerabilities in our applications, websites and networks so that we find them before someone else finds them and uses them against us. So I'm pretty sure Hack the Pentagon is the first of its kind in the federal government and the closest equivalent I can offer to you is the cyber bug bounty program that corporations sometimes now are using. So Microsoft, Facebook, GM and others have used bug bounties as an effective means to crowdsource security solutions at a fraction of the cost and time that it would take to test equivalent solutions in-house. So we're trying this one as well and we're taking a page out of the corporate playbook on this

particular initiative.

In addition, we, like many others, are focused on recruiting and hiring a talent in cyber and other technical career fields in a faster way. You know, we're not known for speed. So we're trying to speed it up. For example, we established a cell of dedicated recruiters to specifically assist in hiring in specialized occupations including cyber as well as some other stem and acquisition fields. So these particular recruiters are now able to use expedited hiring authorities to bring in technical talent much more quickly, which would then avoid, you know, some of the more traditional, more onerous hiring processes. And we've had some good initial results with this one. Since 2014, we've brought in about 1,600 new employees under these expedited hiring authorities and we're hoping to do more of this in the future. So all of this is in the vein of we've got to be more flexible in the way we recruit and maintain some of this important talent.

My fourth and final observation is that because the world of cyber changes so quickly, just like we have to speed it up on the personnel side, so too do we need to speed it up on our acquisition processes. So today we live in a cyber world where companies like Apple and Microsoft can quickly bring forward new capabilities like the iPhone, for example. And then they will iterate to make improvements what seems like on a nearly continual basis. Yet, we and the Department of Defense still sit on top of what I would call an industrial era acquisition process and what we end up doing all too often is we end up giving our airmen yesterday's technology, three years from now because it takes us so dog gone long. So we simply have got to do better.

That's why we in the Air Force started a series of initiatives that we call Bending the Cost Curve. And for those of you who track some of the acquisition approaches that DOD has

been pursuing in recent years, you'll -- you will have heard of the Better Buying Power initiative. So think of our Bending the Cost Curve as complementary initiatives to the Better Buying Power. The goal of our program -- Bending the Cost Curve -- is to do one of three things. And if we're really lucky, we'll get multiples. Either cut our costs, deliver innovation, and/or cut the amount of time required to acquire a new system. So we're looking for one or two or three of those three things under the Bending the Cost Curve initiatives.

So there's a number of initiatives in this vein, but the one I want to report to you on today -- we just announced it a few weeks ago and specifically we unveiled a new acquisition vehicle. So it's a new way that we can put companies under contract. This vehicle is called the Open Systems Acquisition or OSA. And it uses special authority, which is provided by Congress, called the Other Transaction Authority. And the basic deal here is it allows us to create novel business structures that wouldn't otherwise be possible with the standard regulation and it allows us to speed it up.

So OSA is specifically designed to accelerate the acquisition process rather than the normal lengthy period of time it normally takes us. And we're hoping that this new vehicle will give us an average of about three to four weeks from the time we receive a proposal from industry to the time that we award a contract. And for those of you in the business world, you know that's pretty fast. That's a whole lot faster than our norm.

Now we're not going to be able to use this in every regard. Truth in advertising, we're not going to build the next generation of fighter aircraft under such an approach, but we do want to get a start. So what we're going to as a start is we're going to use this vehicle for smaller types of technology insertions and enterprise cyber capabilities. So we are looking to use it in the cyber world.

We did successfully demonstrate the OSA concept last year with our DCGS program. This is a critical communications hub that provides real-time intelligence to our war fighters. And, once again, on DCGS, we found it was taking way too long to deliver upgrades to the program and so we basically tested this approach that I'm calling OSA out in a small way with the DCGS, and, indeed, we were able to deliver some upgrades in a much more quick fashion through that venue. So that's why we created a permanent vehicle and we're hoping that a much broader group of programs will use the vehicle later this year and in the future.

Now in order for people in the industry to get more information or to get involved with this if this is of interest, please go to a website that we've set up. It's called www.transform.af.mil, because we've already listed some opportunities. There's a consortium of companies who are already participating in this, but we would certainly welcome greater participation.

Now as I begin to wrap up and, again, I look around the room, I'm just incredibly proud of what this team and -- including the Air Force, including, of course, the military at large -- I'm really proud of what we've been able to accomplish through collaborative partnerships, collaborative relationships -- and I'm talking here industry, academia. I'm talking to partners like SPAWAR. And, of course, I'm hugely proud of our airmen that I see in the room as well as other members of the military -- members of the Army, in particular.

I was with SPAWAR this morning. Had a great visit. And believe me, they are working hard to deliver cyber war-fighting capability and a whole lot more than that. Just trust me on that. You'd have to kill me I told you any more. But they're working very hard supporting all branches of the military, including us in the Air Force. And later today, I'm going to Joint Base Charleston. I'm going to see our personnel associated with the C-17 and they're working very

hard on their airlift capabilities. And also at the Joint Base, a quick shout out for what we call our P4 initiatives. That stands for public-public and public-private partnerships. A quick shout out to Trident Technical because Trident Technical is involved with one of these P4 programs. This is where we look for a win-win between our military bases and our communities and, specifically, Trident is going to provide maintenance for the base's motorcycle fleet and in return they'll be able to offer classes on the Joint Base as well as allow military to take the off-base course at a reduced rate. So it's designed to be a win-win and be helpful to all of us and we hope that we will get more of these P4 types of initiatives going in the future.

So as you can tell, I'm kind of excited. I'm kind of upbeat about American air power and how the military at large and certainly about strengthening our partnerships here in Charleston. There's a huge amount of important work going on here and on behalf of all of us in the military, we really, really appreciate all of the support that we receive from you in the community. So thank you so much for having me here today and if there's any time at all, I would love to answer any questions you may have. Thank you so much.

* * * * *