2015 Air and Space Conference

Building Cyber Teams — the Inside View

September 15, 2015

MODERATOR: Ladies and gentlemen, welcome to our forum this morning. And the topic is Building Cyber Teams - The Insider View, or The Inside View. We have a wonderful panel whom I will introduce in a moment. And the ground rules are our guests will make opening comments in their free form, and they are not going to bombard us with PowerPoint. They are going to speak from their hearts. We'll continue that as long as they care to make these opening comments, and then we'll open it up for questions and I'm sure insightful answers. And then we need to adjourn here at about 10:40.

We welcome you to Air and Space 2015. We hope that you consider taking a tour downstairs in the technology exhibition floor and learning what industry has to offer us. Today's panel is going to provide insights on increasing demand for full spectrum cyber capabilities and the building of trained and ready teams to defend military networks against attack.

Our panelists include Major General Karen Rizzuti, Mobilization Assistant to the Commander of 24th Air Force; Major General Jim Marrs, Director of Intelligence, U.S. Cyber Command; Major General Ed Wilson, Commander of 24th Air Force and Commander Air Force's Cyber; and Major General Brett William, Retired President Operations and Training Iron Net Cyber Security. So each will make a short presentation, and then we'll open it up for questions. General Wilson, we'll let you begin.

MAJOR GENERAL WILSON: Thank you so much AFA for everything you do. And I'm going to give out a shout-out for Cyber Patriot also if I can get a beer at the end of this. Is that okay? AFA has done a wonderful job really partnering with the Air Force in terms of all things cyber. Just a quick check of hands here in the audience. Does anybody know what Cyber Patriot is? That's a good sign. For those that don't, they outreach efforts public private partnership that has been out touching high schoolers and junior highers. This year, the Air Force Association, in partnership with everyone, is getting into elementary schools making a difference. Last year, almost 10,000 students were involved in Cyber Patriot exposing them to the principles of cyber defense. And so was it a recruiting commercial? Of course not. But I think it kind of speaks to the strategic direction we're trying to take as a nation. And AFA, they are really the frontrunner there. So just hats off to the team. Not just for that but for everything that you're doing for the Air Force.

So I’m Ed Wilson. I live down at San Antonio, Texas where the team gets paid to worry about cyber every day for the Air Force. The topic is cyber teams, building the cyber teams. So if I say cyber mission force in this audience, I'm going to do a quick poll to see if I say cyber mission force who knows what that is? Pretty good. About half the team does. About half the team doesn't. That was a decision —— it was a decision made approximately three years ago, about two and a half years ago by the nation to stand up approximately 6,000 people dedicated to three basic mission areas; one, defense of the nation, two provide quick comm support in terms of cyber options, both defense and offensive and then, three, defend cyber terrain. And so each of the services has been at it very hard over the last two and a half years.

For the Air Force, we're about halfway through our build. 1,700, 1,715 operators in Intel analysts, et cetera, dedicated at -- I would describe it as a cyber-maneuver force that the Air Force is presenting into the joint construct. A total to include training, (sustain eval) first sergeants, that kind of overhead, roughly 2,000 people across our Air Force that have been added, new billets and people coming into this mission set. It's the additional capacity and capability we're adding to the team, very joint in nature. So we are partnered up with U.S. Cyber Command to build that. We're beginning to now see the difference those teams are making, both defensively and offensively in terms of options that are available. I think the Air Force is doing a magnificent job. We have really approached this from a full dot mil PF, if you will, approach. We have schoolhouses that are up and running training our cyber defenders in particular, as well as some of the offensive capability that is bringing some real measure into making a real difference. We're seeing it today.

I was just comparing notes with Retired General William. When ET was part of the U.S. Cyber Command Team, a lot of things were on PowerPoint when it was being briefed to the tank, and it was a concept in nature when you walk out on the floor. General Welsh was just down for a visit about three weeks ago, and I think he was taken aback by how far the team has come. Things that were PowerPoint deep that were concepts in nature, today when you walk out on the floor they're for real. There’s real teams on real systems doing defense of not just networks but mission systems, things like your operation centers, things like command and control systems for satellite systems, et cetera. And so that's a positive report from that vantage from today. Does that mean that we're finished? By no stretch of the imagination. We've got a lot of work to do.

So when you look at our basic lines of operation in terms of network operation, I think we're doing really well there. Defensively, we're doing very well. I think some of the constructs the Air Force is running as half cyber in support of cyber command is very effective. When you look at the things that we need to be doing, there's a lot. And it's primarily associated with the defense of weapon systems and installations around our Air Force. How do we bring the five core missions at our Air Force in support of air component commanders? What's the role in responsibility for those that sit on the team? And so I won't get into the details. My guess is we got a lot of questions in that arena. But I'm proud to serve, and I think we're doing magnificent work. And it takes a whole team. It's not just 24th Air Force.

And so with that, I'll wrap up and pass it off to Karen Rizzuti.

MAJOR GENERAL RIZZUTI: Good morning. Karen Rizzuti. And I just left the 24th Air Force as the MA there and looking forward to transitioning to U.S. CYBERCOM. I appreciate the opportunity to highlight the total force integration that has been going on in cyber for a long time. This is nothing new. The Reserve had been integrated across the board in cyber defense, network operation squadrons, the operation center, and the Guard as well, very well integrated. As a matter of fact, the Guard is the predominant force with combat communication and engineering relation. So TF integration and cyber business is nothing new.

We also have on the Reserve side individual augmentees or IMAs who are throughout 24th Air Force, MAJCOMs, joint agencies like DAA, DISA at the unit level, so our individual mobilization, cyber experts are also hard at work all over the place. So initially when it came time to build cyber mission force, the Air Force integrated the Guard and Reserve into that concept. As a matter of fact, more so than any other service because they are an integrated part of the 1715 that General Wilson mentioned. And that com—build is a total force com—build to bring on the cyber mission force. It included a Reserve squadron for cyber protection teams integrating with three active duty teams [inaudible].

In addition, the Guard is building 12 cyber protection teams that will make up two full—time continuous protection teams, and they'll be mobilized on a rotating basis in order to fill that requirement. And the Guard is also building units to provide a portion of the national mission team, cyber portion of the national mission team again on a rotating basis. Nothing new and even the joint force headquarters part is planned to be integrated. We've already got augmentees there and are planning to plus up the augmentation unit at our 624th operation center, complete TFI operation.

So why is this important that we work as a team?

This mission doesn't get done on a daily basis without all three components. Well, it's important for several reasons. I just want to highlight a few. The first one being to retain that talent, train and ready airmen that decide to get off active duty. We want to retain those trained folks, and we want to continue to use them in uniform as they will often work for civilian companies. We want to make sure that we keep the talent in uniform. Another thing is we want to take advantage of their industry connection, so when they go out and work for these commercial companies and they put their uniform on and come work with us part time, those connections and those relationships are extremely important. And they are —— as they stand at these units, and they all become fully manned and trained, they are providing great additional capacity that we can use that we can call upon in time of crisis or emergency. And I do want to emphasize the key there is that everyone —— this is how we do it in the Air Force. Everyone is trained to the same standard and the same certification process. So there is no tiered readiness in the Air Force. We are all trained and ready.

Additionally, we talk about to how this has to be a whole government, whole nation approach in cyber. These partnerships are so important not just with industry, with academia, with our allies, extremely important that we maintain these relationships and that we stay on the leading edge of the thinking that's going on in places like Silicon Valley, and so we've got some initiatives going on there. So I think just to wrap it up, the bottom line is we don't do the cyber mission without all three components every single day and going forward. I think as future requirements come on line, the Air Force will nationally make it a total force enterprise with regard to requirements. If we don't –– we gain tremendous benefits by working together as a team. And honestly, what's made that work has been great leadership. I know we'll do that moving forward.

MAJOR GENERAL MARRS: All right. Well, thanks, Karen. Good morning everybody. I would say, Bernie, thanks so much for the opportunity to be here this morning. I will set the record straight in fairness to my colleague, Brigadier General Mary O'Brien, who is currently the CYBERCOM J2. She is very much an upgrade in the position. I, unfortunately, for those of you in the space business, failed to achieve escape velocity, so I am back in the Pentagon now, but I am forever indebted for the chance to get out of the Pentagon for a few hours. So thanks a lot, Bernie.

What I want to talk to you about for just a couple of minutes is former CYBERCOM J2 is really not so much the threat. And I think everybody here is, I'm pretty sure, familiar with the fact that we're dealing with an unprecedented volume and velocity of threat out there that spans the range from individual hacktivists up through nation-state actors, but I think this group is together today to figure out what we, and specifically the Air Force, are going to do about it. And so I'll go very briefly through a couple of things that hopefully will help generate some thoughts and make this more of a discussion as we go along.

By the way, it's great to see all of the blue out there. I've been doing the joint thing for a while, so this is very nice to see. Thanks. I will start with a non—Intel comment and say that first and foremost over many assignments, I have been a consumer of cyber talent and cyber skills. So one thing I can tell you is that we don't have nearly enough —— as amazing as our team is out there, we most definitely need to figure out a way to generate a predictable and larger supply of motivated cyber professionals out there. So I will say for Bernie and for AFA and the Cyber Patriot program out there that that is absolutely what we need to be doing is identifying folks early on who have that inclination not only to do great things in the cyber world but to marry that up with their interests in doing something for their country. So thanks for that.

Just two things I'll hit on really from my time at Cyber Command in addition to just dealing with the world day—to—day and making sure that Cyber Command was doing that well informed about the threat. What we spent an awful lot of time thinking about was whether the cyber mission force as it begins its exponential build—out had the all-source Intel to do what it needed to do. And so that took an extraordinary amount of time and attention from not just the Cyber Command team but the cyber component Intel teams out there as well and the larger Intel community to figure out how we do that. So a big part of that magic was as these teams began to form, we introduced them to colleagues within the Intel community that were familiar with those target sets. And it just was a way to start thinking about various ways that they could be more effective in the mission that they were assigned.

Second, we spent a lot of time also helping to foster the cyber intelligence capabilities within the defense Intel enterprise. So as nascent as this mode of warfare and this domain is, a lot of what we were doing along the way was to help the IC make connections in terms of who's specializing in what and making sure that that talent was available to the cyber mission force teams as they moved forward. So what does that all mean for the Air Force? I think there's a very, very good discussion going on within the Air Force right now about what does cyber mean to kind of the five-point mission areas within the Air Force. And I think that's a healthy, very healthy discussion to have right now. All of the services need to figure out both how much they're able to support the joint fight at large and what the cyber dimension means to everything else that they do out there. And so I would just say that the Air Force has been a fantastic partner on the Intel front, and I think is doing a nice job of ponying up to Intel analysis response responsibilities that make sense for Air Force cyber mission. So a lot of great work going on at basic as an example of making it happen. So I look forward to your questions, and I think I'll turn it over to ——

MAJOR GENERAL WILLIAM: Thanks very much.

First of all, I'd like to thank AFA for letting a retired guy come up here and say a few words, so I appreciate that very much Bernie. And Bernie said you'd get a beer if you mention Cyber Patriots or Cyber Patriot, and I will also offer a beer because I want to compliment everybody on the excellent judgment they had to come over and listen to this discussion on cyber teams as opposed to that boring thing that General Carlisle is doing next door on 5th Gen warfare or whatever. So I will give a beer to somebody if they will go up to General Carlisle and say, hey, sir, that was a great talk you had today. I tried to get into the cyber thing, but it was full, but I enjoyed yours anyway. Let me know how that goes.

For those who don't know my background, my short bio is I spent 28 years in training as a fighter pilot before I got into the cyber and comm and IT business. My first job was as the J6 at PACOM, and then I finished up as the J3 at Cyber Command. It was an interesting transition to go from that world when General Howie Chandler called me and said, you're going to be the J6 at PACOM. I'm like, excuse me, the J what? And it was the J6 at PACOM. But it started me off on something that has been extremely enjoyable and that I've really enjoyed working with. And this issue of training and teams and all of that is extremely important to me. And it's very satisfying to hear not only the discussions here but I shared with General Wilson —— I had the opportunity to talk to the Chief a couple of weeks about, and he talked about his visit out to both 24th and 25th Air Force, and he's going, yeah, and it was so cool. He says, they got this AOC thing there, and they've got this cyber air tasking order, and it's got the teams listed, and it's got all of this stuff. And I was just thinking back to the first time I briefed the Chief on all of these concepts which was in the Fall of 2012 right after he became the Chief. And then about six months later, I briefed the Joint Chiefs of Staff trying to get the money to fund these teams and all that sort of thing. And I can tell you in both of those, his body language was not the same as it was a couple of weeks ago when I talked.

You remember at that time he was talking about, is it a big C, is it a little C? I don't know if this is a black hole, any of that kind of stuff, which is all the questions you should be asking if you've the Chief of Staff before you commit resources into approaching not a new area of warfare but approaching an area of warfare in a much different way, I think, than we have before. So to me, it's very cool to see this growth in things that like General Wilson said really started on a white board back when I was at PACOM some of these thoughts, and they advanced to PowerPoint which was good. But now to see what the Air Force has done as part of the joint force to really implementing this and making it happen is very satisfying. So to all of you that have been working this, I compliment you. It just goes to prove what I learned the first time I was in the Pentagon, that all the gut ideas have a gestation period. And so I think the gestation period is starting to come along.

I just want to hit on two other things real quick. One of the first discussions I had with General Alexander who was the commander of CYBERCOM. When I got in there as the J3, I said, you know sir, you're real good at setting a strategic imperative for action, and there are a lot of threats out there and nation states and all of that kind of stuff. And then he's very smart technically, so he could talk all day about how many people it will take to get through this, you know, encrypted firewall or whatever the case may be. But I said, if we're going to become a command, if we're going to treat this like an operational war fighting domain, then you got to put things in between those two like command and control and a force structure and an operating concept and resources and that sort of thing. He goes, yeah, I know, you need to do all of that. And so eventually, you know, with a great team, we have seen this come to fruition, and so it's very cool to watch this happen to see the command and control, the force structure and the doctrine to develop with this.

One of the things I think is really important about training, we are talking about training the cyber teams, is there tends to be a lot of focus on the tactical and the technical level of training which is extremely important. Just like any career field you start off in the Air Force, there's a level of tactical and technical expertise you have to have. I would argue with cyber space operations that when you get to the operational and strategic level that there's much more in common with what we already do than is different. Tactical operations in any domain, air, land, space, maritime, the tactical operations are different, but how you integrate those as a joint force at the operational level becomes extremely important. So the way we're starting to develop the training at the operational level, I think, is extremely important. And we got to think about how that gets integrated from undergraduate education, whether that's at the Air Force Academy or someplace else, what happens at the weapons school now that we've stood up the cyber weapon school and how that gets integrated, what are we doing at Air Command and

Staff College, at SAS, at National War College.

I know General Kwost is standing up some new cyber educational concepts. So all of those things start to complete the picture that allows us to treat operations in cyber space like operations in any other domain and truly to bring those together as a joint force. So I would encourage you as we think about training these teams we should also think about how are we training the next J3 at Cyber Command? So like I was a fighter pilot. The guy that replaced me was a submarine driver. I always said when I was in that job I want to see the point where we don't take somebody from another operational domain, that we've grown people who have seen cyber space operations as an operational domain, and those people grow up into those leadership positions, and so I would encourage you to think about that.

And the last thing, I just wanted to pick up on what General Rizzuti said about the total force because we did a couple of exercises at CYBERCOM. Cyber Guard was one of them. But this integration between what's going on in the private sector and what goes on in the government, specifically in the military, and being able to read those two off is extremely important. I can tell you I haven't been in the private sector for a little over a year. There are some good folks out there, but they don't have what I would call an operational approach, an approach that says, what I do really use cyber space for? In the military, it’s command and controls, to get information, move information, use information, to make better decisions faster than the enemy. And so you have to prioritize the protection of that in a very specific way. And talking to General Wilson, that sounds like exactly the focus that he's bringing to the 24th Air Force. So the civilian community doesn't get that as well.

The other thing that the civilian community doesn't get is that –– well they get it, but they don't have access to it. Right? There's three things you have to do you have to defend your networks. You got to hunt for bad guys that get in there, and then you got to have the ability to go kill the archer. Right? You got to have the ability to stop the attack before it gets to you. And that's something only we're authorized to do. But bringing that mindset and sharing those thoughts back and forth between the Air Force and the civilian community through the Guard and Reserve forces, I think, is extremely important. And so with that, I'll stop talking. But again, I appreciate the opportunity very much and look forward to your questions.

SPEAKER: Well, thanks. That was very insightful. Let us start very quickly with questions. And we have about 20 minutes. This first one is directed to General Wilson. And the question is, do we have Title 10 right to mold that mission? To organize, train, and equip of course has been the mainstay of how we do things as a war fighting force. Does it apply in a linear way to cyber, or do you think there may be some modifications that need to happen?

MAJOR GENERAL WILSON: So the context of

that question typically is in the mix of Title 10 and Title 50 especially when your comm to offensive cyber operations is typically the context. I think today's construct works —— the challenge is not to get ourselves wrapped around the axle with regard to authorities right out of the shoot. And the language we typically hear is, these are Title 10 forces, these are Title 50 capabilities, et cetera. I think we need to back up. And it gets back to the operational heart that DT William is referring to is what are the effects that we want to deliver on behalf of a command route, whether that's a COCOM air component commander, what capacity and capabilities and expertise in terms of operators involved human capital involvement, capabilities from a technical perspective are required to deliver that effect then we put in place the right authorities to execute those operations so that we have an exhort in hand, and we're leveraging both Title 10 and Title 50 capabilities and authorities. And so we do that today. And it's refreshing to be honest to be able to talk about the fact that we conduct offensive operations when directed. It's in our DOD cyber strategy that's been published. And so to be able to sit up here and actually reference the fact that we've been chartered as the DOD to provide that kind of capability for the president, for the secretary of defense is good.

So from a Title 10 perspective, do we have the right set of authorities? Absolutely we have the right set of authorities. Could we take a fresh look at the Code, the U.S. Code as this matures in terms of a mission set? Absolutely. And I think that gets back to ET referenced it, you know, we've moved from PowerPoint into actual operations. Today we don't see that as a tremendous constraint today assuming the rights of authorities.

SPEAKER: Thank you. General Marrs, some of us remember the transformation of intelligence from a paucity of information which was the big challenge, how do we get out and learn more about the bad guys, to a glut of information about the bad guys. And the challenge in the intelligence community became how do we manage all of this, how do we parse through it to get something actionable in thinking in terms of other forms of intelligence. What do you see as the construct right now for cyber intelligence? Is it too much stuff and the challenge is managing that, or is it going out and finding the stuff that we need to manage so that we give it to the war fighters to do what needs to be done?

MAJOR GENERAL MARRS: Great question. I would say it's actually a little bit of both. Part of what we're finding is that obviously with just the quality of network activity around the world just understanding what's going on and trying to sort through that is a tremendous, tremendous challenge. A big part of it is actually being mindful of what's going on in the everyday open source environment. And I think that's something that we're rediscovering along the way is that there isn't as much magic to this as you might think, but it does require very much still being on top of that.

I think in terms of how we share that with the operational organizations out there is a work in progress right now that all-source organizations such as DIA are still working through evolving their cyber all—source analysis capabilities out there. Others like NSA have been living this for years and years, but there's still a difference between kind of traditional NSA missions and what we on the cyber side of the house need day in and day out. So it's a little bit of digesting the volume and a little bit of tailoring that for [inaudible] and we're making good progress.

SPEAKER: Thank you. General Rizzuti, many of us are familiar with the terms Associate Unit and Reserve Associate Unit mixing and matching active duty aircraft and ART crews. You mentioned in your opening comments formalizing partnerships with industry. You mentioned the value of having members of the ART be full time in the IT industry. Do you see any need for constructs that more fully leverage those capabilities, is it sufficient to have IMAs that are accessible to you from industry, or might there be other relationships that could be explored with industry itself directly to the department?

MAJOR GENERAL RIZZUTI: Well, that's a great question. And it isn't just individual augmentees that we use that are working out in industry but across the unit program as well. We have folks that every day are working in commercial enterprises, some pretty high up at the executive level in some of these companies, and they bring this expertise to bare. But there are a lot of discussions going on and some new initiatives, especially out in Silicon Valley which I think will grow to other areas to other centers, academic centers. This one, this point of presence in the defense, innovation unit, experimental in Silicon Valley are just the beginning. We're trying to cement relationships on an ongoing basis, I think what you're talking about, so that we have folks who already have these relationships between military and industry, and we're growing those, and we're trying to make central point of presence for that interaction because there's a lot of different organizations across the DOD and other agencies that are kind of descending on Silicon Valley and want to build these relationships. So I think establishing these programs is a great thing, it's a great start, and it's only going to grow from there.

SPEAKER: Thank you. General William, we're blessed to have with us someone who has done the fighter pilot thing and then done the cyber thing.

MAJOR GENERAL WILLIAM: [off mic].

SPEAKER: Well, I understand. There's been an evolution in weapon systems over the past probably dozen years or so where they have gotten incredibly complex, incredibly networked, and in a very real way cyber dependent, in particular unmanned aerial systems. Would you please spend just a couple of minutes describing what the vulnerabilities are of that and how you think we ought to mitigate that risk as our even manned systems become more dependent on network?

MAJOR GENERAL WILLIAM: The vulnerabilities are clearly out there, and there's parallels to the discussions you see in the media about threats to critical infrastructure whether it's power, water, telecommunications, those kind of things. And all of those things were built without the idea that somebody was going to attack them through cyber space. And same thing with our weapons systems. While there's certainly, and of course I'm not exposed to it now, but I see the discussions in the media where more and more we're thinking about the F-35 and thinking about how do we defend that within the domain of cyber space. But most things about the F-35 were designed well before we started thinking about a threat through cyber space.

So General Wilson and I were talking earlier, and he's really focusing, I think if I had that correct, that the cyber protection teams to a certain extent on these mission systems. And there's a wide variety of those. There's those that do command and control which arguably are the most important because you can have all of the cool weapons you want, but if you can't command and control them it doesn't do much good. So protecting our AOCs, making sure the ATO gets to the right people in its original form, it doesn't get to the other people, things like that. And then all of this tied to the weapon systems. I remember several examples when I was still in active duty with things that had happened with maintenance laptops, for example, that become connected to airplanes. And so what it really highlights is everybody, not just the cyber people, has a role making sure that these mission systems are secure and so the policies and the governance and the things we design in to make sure that the users execute things correctly is extremely important. But I think you're exactly right, this focus on mission systems is fundamentally important.

SPEAKER: Thank you. This is for General Wilson and General Rizzuti. There are many elements of the US Code, Title 18, Title 32, Title 10, Title 50 that all kind of come together. And we like to talk about how seamlessly integrated we are as a total force. Rather than just ask you whether or not we are, please describe for us in turn whether there are things we can do better to better integrate the total force in this critical mission area.

MAJOR GENERAL WILSON: So I guess the best way to describe it is I think we have a very well integrated team today, so much so that if you were to walk out at our [inaudible] our defensive enterprise defense for the network, you would see total force blend. If we did a show of hands, there was a mixture of people there both in a classic associate relationship. There is Air Force OSI that works hand in hand on a 24/7 basis so from a Title 18 perspective. And so we have integrated into the fabric of how we operate the network and then address the threats that are placed in our Air Force every day in, I think, a very agile sense to be able to handle the right set of authorities, the right set of actions to be able to accomplish what we need to do, whether that's a law enforcement action, a counter intelligence action, or just with the natural network operations in defense of the network that go on day—

to—day.

So to be candid, I don't see a tremendous amount of seems right in today's structure. One of the challenges ahead of us, I think, is we build up the cyber mission force. There's definitely the total force presence there. One of the items that are beginning to come up from a legal perspective is the ability of the Air National Guard and the Army Guard, National Guard that are both field in the cyber protection teams as part of that force. That force structure is when they're not in Title 10 capacity executing day—to—day operations and they're back in their respective state, can those things be used for in a Title 32 capacity? The answer is of course they can.

Now, the next question is as we provision them with equipment that has been paid for out of active duty POM assets, et cetera, can they use those in a state capacity? I think the answer is still yes, but we're working through some legal reviews of that just to make sure that nobody is speeding. I think it gets back to we need to grow more capacity as a nation. It's not just in the Air Force but as a nation to be able to respond to strategic threats to the nation. And so we see the Guard and the Reserve and the active component as part of that response, that capability that we need to build. But today, again, I don't see tremendous friction or constraints associated with the current US Titles. We get the job done every day without it. I think in the future we build more capacity, but we may need to take another look at the Codes.

SPEAKER: General Rizzuti. And you need not be quite so diplomatic, but that's okay too.

MAJOR GENERAL RIZZUTI: No, I would have to agree watching how operations are done every single day. It is blended operations, definitely three component ops, more so than I have seen anywhere else that I have worked. There are challenges. I mean there are some challenges, not necessarily with the title. I think we've worked through all of that. And as we do standup cyber mission for cyber protection teams, those folks are going to be in a Title 10 status when they're working for 24th Air Force for CYBERCOM. Other challenges include we’re all building force at the same time, so it's a building challenge. It's getting everybody through training. It's getting everybody on board. It's more —— that's more the challenge, I think, than the title issue.

SPEAKER: Thank you. General Marrs, we hear often of strategic intelligence and operational intelligence. That's very understandable at the [inaudible]. It was very understandable in the [inaudible]. Do you think that the definitions of strategic intelligence and operational intelligence may have morphed or need to morph in the context of a global cyber domain?

MAJOR GENERAL MARRS: As in many things, yes and no. And I will say that I think they do need to change from the standpoint that cyber is unlike any other domain in the sense that you have friendlies, adversaries, noncombatants literally living within the same server. And so what could be taken as a tactical action by somebody or conceived of as a tactical action could have strategic implications in terms of who it affects, so I think we all need to be cognizant of that.

That said, in terms of how we think about war fighting are kind of the fundamental building blocks if you look at how a combatant command thinks through adversaries out there and what it is that we need to be prepared to do. Some of that fundamental framework still very much applies. So within the Intel trade and within the planning business, we put together things called JIPOE, Joint Intel Prep of the Operational Environment. That's kind of the foundational product that planners within the combatant command use to wrap their brain around the threat that's out there and what do we need to do about that. So CENTCOM does that every day, PACOM does that every day, Cyber Command does that every day. What's different now is the cyber layer within that JIPOE that takes place. And then there are finer grain versions of that as we work down to more of the operational level and actual cyber mission force teams. So a lot of sort of tried and true trade craft that still applies but in a very, very different sort of way.

SPEAKER: Thank you. We have time for one last question among the many that I've been handed. This one is for General William. Now that you've seen things on the uniform side and you're seeing things on the industry side, we'd be interested in your perspective on the acquisition of new technology and rapidly bringing new technology into this cyber mission set. It's quite one thing to develop a new processor chip and to develop a new jet engine technology and bring it in, and that's a very deliberate process, but it seems that we're all familiar with people out on Hacker Way and Palo Alto who can turn out something quickly. What is your assessment of the ability of the department to incorporate rapidly evolving software techniques and other tools that would be useful in this important and additional area?

MAJOR GENERAL WILSON: I definitely think some of the initiatives that Sec Def has pursued and were mentioned earlier with trying to work with Silicon Valley and that sort of thing. But frankly, my experience working the Air Force budget, we had the same problems that –– I've worked with a number of large companies with very large budgets, and they just –– the organizational bureaucracy is not structured in a way that allows them to take advantage of next generation technologies. What you see with companies now –– Sony is a great example. You get hacked, you have a big thing happen, and you go throw a bunch of money at the problem, but I'm almost sure that they're throwing a bunch of money at the same kind of stuff that other people have in place that they're getting hacked with. So you have got to devote –– you've got to devote some part of your budget to leading edge technologies. And one company we worked with, the CISO, the Chief Information Security Officer, had 20 percent of his budget that he was allowed to allocate to leading edge or bleeding edge technologies. So he, all the time, was experimenting with something new. And so I think we've really got to continue to focus on that. That's beyond even a DARPA type of thing. I think it's something that you put in the hands of these people that really know how to use this. Try it out. If it works, buy more of it. If it doesn't, go on to the next one. So I think it's got to be a pretty big philosophy change.

SPEAKER: Thank you. Again, many, many more questions came, and I will allow our wonderful guests today and speakers today to address them as they can as we adjourn. Let me remind you that AFA is devoting significant energy to cyber things. And one of them is happening September 22nd and 23rd up at the University of Massachusetts in Lowell, Massachusetts where we'll be hosting an AFA cyber workshop, and full information is available at our website. Again, I would invite you all to make your way down to the exhibit hall as you can because there are many good things to be seen there. Not the least of which is a wonderful AFA booth with comfortable chairs and a half-priced discount on AFA membership. Help us keep these things going. Please join me in thanking our wonderful panelists this morning and have a great rest of the conference.

* * * * *