Lieutenant General Michael Basla
Lieutenant General Robert Otto
Major General Brett Williams

AFA - Air and Space Technology Exposition

"Cyber"

17 September 2013

Lt. Gen. Basla: Scott, thanks very much, and ladies and gentlemen, thanks for participating with us this morning. Thanks to the co-members of this panel, my great friends actually Bob Otto and Brett Williams.

Scott, in order to answer your question, the longer your duty title the less important your responsibilities are.

Thanks to AFA. Thanks to AFA for sponsoring this great event. What a wonderful event for our Air Force and our nation here in the capital.

I just want to provide a few opening remarks to give context to today's discussion. As Scott said, I'm the Air Force CIO and Chief of Information Dominance, but I don't do this alone. I work with many partners in our Air Force including Air Force Space Command.

We have different responsibilities to deliver cyberspace forces and capabilities to our Air Force.

As Chief of Information Dominance and Chief Information Officer I'm charged with advising Air Force leadership and directing Air Force strategy and policy for how we employ information capabilities and develop cyber airmen. To that end, my office and team provides the Air Force with strategy and policy on how we deliver information and information technology capabilities to our warfighters. We ensure Air Force IT capabilities are designed to support the Air Force mission, all the missions, and effectively integrate with the joint community, with the overarching strategic objectives of achieving our five Air Force core missions -- air and space superiority; intelligence, surveillance and reconnaissance; rapid global mobility; global strike; and command and control. And everything else underpinning that in order to deliver the capabilities in those five core competencies.

As the Air Force cyberspace functional authority we work with Air Education and Training Command to develop the curriculum and the professional development programs for the Air Force cyberspace operations and support peripherals.

Air Force Space Command holds responsibility for both space and cyberspace which includes serving as the lead command for cyber

weapon systems as well as the core functional lead integrator for space and cyberspace. Air Force Space Command is responsible for organizing, training and equipping our cyberspace forces. Under them they have the 4^{24th} Air Force and that's the numbered Air Force that executes Air Force cyberspace operations and support activities. They also serve as the Air Force component to U.S. Cyber Command as AFCYBER.

Today my team in the Pentagon is developing strategic guidance for the Air Force information environment. A strategy to put us on the path to align our IT efforts in all areas. Especially in today's fiscally challenged environment, our IT initiatives must optimize every dollar and drive the balance between security, capability at the best value possible.

There's a delicate balance between efficiency and effectiveness so we have to apply good operational risk management and strive to provide greater IT capability to our warfighters with cost in mind.

In addition, we'll strive to optimize our guidance on warfighting integration and corporate process roles.

We're looking for the right places to insert the CIO in the requirements, acquisition and budgeting processes that exist in our Headquarters Air Force. In the Pentagon I sit between the A3-5 and the A2, and I'm in a good position to advocate for not only their informational capability needs but throughout our Air Force. We can develop an information environment to serve as the foundation for their and other information technology requirements. We'll drive the development of Air Force information system to establish standards and help shape the joint information environment. The JIE will serve as the target for the joint warfighters' basic information needs and the Air Force will be part of that.

The Air Force will look for areas where we can take the lead in shaping the JIE and will take a supporting role in areas where it makes sense to follow. Our warfighters can still develop and employ their unique mission systems needs, but these too must align to common security and architectural standards of the Air Force in the joint information environment. This is foundational to integrating joint warfighting capabilities.

In the past year despite sequestration and our tighter fiscal environment, the demand for full spectrum cyber capabilities across the department has increased significantly. The Air Force alone has been tasked to provide another 1264 additional cyber airmen to meet U.S. Cyber Command's needs. The Air Force is

focused on developing cyber airmen with a wide breadth of cyber knowledge and to ensure we prepare our cyber professionals.

We've got an undergraduate cyber training program under AETC that's fantastic and we've developed -- and I'm running out of time here -- a cyber weapon instructor course at Nellis under Air Combat Command and the Air Force Weapon Center.

But let me tell you, all of these programs are not without challenges. I've already mentioned the fiscal challenges. I've already mentioned the environment in which we have to operate. But to tell you the truth, we have some great partners in which to do that.

I'm really pleased to be here and I look forward to your questions. Thanks for the opportunity.

Lt. Gen. Otto: Mike ran through quite a bit about where we are moving in cyber and what's pretty obvious is that cyber is in a period of transition. That word comes up a lot these days about being in transition. It reminds me of my friend Tom who just retired and got a job in cyber. Second career. But he just couldn't seem to get to work on time. Every day he was five minutes late, ten minutes late, fifteen minutes late. But he did great work. He was very detailed. His boss enjoyed the product, but he felt he had to address the on-time issue.

So he called him in one day and he said Tom, I like your work ethic, I like your product, but you've just got to get to work on time. He said boss, I'm working on it. I understand that's a problem. His boss aid I'm glad you acknowledge it, but you're retired Air Force. Why is it that you can't do this? What did the people say in the Air Force when you came into work late? He said, well, good morning, General. [Laughter].

So I want to say good morning to all of you, and I also want to thank Scott Van Cleef and the AFA for hosting this opportunity to talk about cyber.

The theme that I want to talk about are not the specifics, since Mike covered that, but ISR -- intelligence, surveillance, reconnaissance -- is really integral and essential to cyber operations, probably more so in the cyber realm than operations in any other domain.

The first point I would make is that operations in cyber is not really that new. In the ISR world certainly we've been dealing with it for a while. So even though it was 2011 that the Department of Defense labeled cyberspace as an operational domain, remember it was back in 2005 that the Air Force added

cyber to our mission statement. Talking about fly, fight and win in air, space and cyberspace. So if you look back from that incrementally by decades, it was the decade prior to that, in 1995, that the Secretary and the Air Force established the definitions of information warfare. Then you go back ten years prior to that, 1985, to really discover the Air Force's inception in cyber.

The first known incident was an OSI agent who was intrigued by a call that he got from an astro guy who had turned into a CISAD at one of our FFRDCs and he had found intruders into the network in the national lab. The Air Force got involved through OSI and they helped unravel what ended up being an international espionage ring. It was nicknamed Cuckoo's Egg. What it was was German hackers who were trying to steal classified material on the SSBI, the Star Wars initiative, and then they were selling it to, at the time, the Soviet KGB.

So if you think back what was happening at that time, that was when computer security or COMPUSEC was under the Electronic Security Command, a predecessor to today's Air Force ISR agency. That evolved into the various capabilities that we recognize today as cyber operations. Offensive cyber operations and defensive cyber operations.

I don't know of Major General John Cassiano is here. He was here yesterday, I ran into him. When he was in charge of the intelligence agency in '96, the first combat cyber unit fell underneath his command and it was the 609th Information Warfare Squadron. And so they were at Shaw Air Force Base, the 609th, and established to support CENTAF with their combined offensive and defensive cyber missions.

So this is not new stuff. This was the unit that gave us the term INFOCON which is still in use today.

Mike talked about it. The JCS has approved a rapid growth in the cyber mission forces. When we neck this down to what the Air Force is going to provide, the bogey is 1264 large growth in Air Force cyber. What you may not know is about half of those teams are intelligence, surveillance, reconnaissance airmen. Then it's about 60 percent of the outside the net teams.

So why is that? Why is the composition the way that it is? And although it's a completely over-used analogy, if you think about that iceberg, the people that are actually on-net are that tip of the iceberg sticking out of the water, but there's a tremendous amount of support that goes on underneath the water that is unseen, but it is that expansive intelligence, surveillance and reconnaissance operations that are required, doing that intensive

analytic work that leads to the operation itself. It's not just on-net stuff, it is all the other INTs. Human intelligence, geospatial intelligence, signals intelligence, open source intelligence. All of that wrapped up in order to inform the kinds of operations that we need to do on-line.

So I would say that the intelligence aspect of cyber operations takes an incredible amount of preparation work and study in order to create results. That comprehensive intelligence on difficult to access targets, just the networks, the actors, the capabilities, is extremely manpower and man hour intensive. But it needs to be exquisite in order to effectively defend our networks, go after some of the more difficult things that we face out there. So if you kind of measure that out as a percentage wise, something like 90 percent of the operation is the ISR portion of this. That amount that's underneath the water.

So that takes a very large, takes a very specialized cyber team to support that. Then when you talk about the operation itself, if you think about kind of a pilot and a copilot, that copilot is going to be an intelligence, surveillance, reconnaissance trained airman.

What are we doing about it? As we built up to this 1264 airmen, we're also working the details on an Air Force cyber strategy and I would say that we share a common vision of what we need to do.

Certainly as Mike Basla mentioned, we need to build and maintain and assure our Air Force network operations. We need to optimize our capabilities for the joint fight. And we need to enable our Air Force enduring contributions of air and space superiority, mobility, global strike, global ISR and C2. It's that last aspect I think that we're going to see a lot more progress in the future in an area that we see more focused.

So I would say simply that this is an exciting time for cyber. Certainly it has the nation's attention. It's clear if you follow what's going on in Congress that it has Congress' attention and discussion right now. And now we're seeing this third piece about the military planning that's absolutely essential in this domain.

The nexus of those three things I think means that we're going to see a tremendous amount of progress in the next couple of years, irregardless of the Snowden incident. And we look forward to that debate.

So I just want to thank you all for the opportunity to talk about cyber and anything that might involve ISR as it relates to that.

Maj. Gen. Williams: For those of you that don't know me, I spent 28 years in training as a fighter pilot to become a cyber guy. I was sitting up at Kadena as the wing commander and get a call from General Chandler and he says hey, you're going to be, you're going to work at PACOM and you're going to be the J6. I'm sorry? What did you say?

So I spent a year and a half as the J6 at PACOM which was a great experience, and I've been at CYBERCOM for about the last 13 or 14 months.

Where I find myself is between people that understand operational art, or think they do; and then people that understand cyberspace stuff at the technical level. So I have no credibility with these people because I'm a fighter pilot; and all these people think I've gone to the dark side and all they hear when I talk is [Eco watts] per fortnight. So I find myself working between those two.

But what I'm going to offer to you is, I haven't done this now for about four years. I've got four I would call them axioms, but not everybody would agree they're true, so I'll just say they're four conclusions I've come to about cyberspace operations, and then three of what I would call, from my perspective as the J3 of CYBERCOM, technical gaps that we really need to fill as quickly as possible.

The four conclusions I've come to is that number one, I don't think it's productive to talk about cyber war. I think that war, conflict, competition, there are enduring principles in there and cyberspace offers another domain, another environment, whatever word you'd like to say, to be able to exercise the elements of national power. If you talk too much about cyber war you end up ignoring the fact that at the strategic and the policy level that you have to put cyberspace operations within the context of the dime fill, within the context of the whole of government approach, and you've got to think about how do I leverage cyberspace to achieve my national security goals.

The second conclusion would be, following on from that at the strategic level when I come to the operational level that the more I learn about cyberspace operations and the more I reflect on what I understand about operations at the tactical operational strategic level, the more I'm completely convinced that the operational level, everything you read in Joint Pub 3.0, operations; everything you read in Joint Pub 5.0, planning; everything you read in Joint Pub 3.60 on targeting; that all of those processes, everything we've developed as the best way to do things in doctrine, I can show you how cyberspace operations fits in that just fine.

So while we've done a good job of telling people how complex and how different and how mysterious cyberspace is, at that operational planning level we can execute it a vast majority of the time with the processes we've developed and the processes that have worked.

Number three. If you're going to do what I just said in number two, then you have to train cyberspace operators. You have to train people that understand cyberspace operations at the tactical and technical level so that when they come into that joint staff and they're operating at the operational level they can bring all of that together in a relative and meaningful way. Which is why if you go into any joint staff J3 or J5 you find soldiers, sailors, airmen, marines, they all bring their domain expertise into that level of operational planning and then they're able to bring that together to satisfy the combatant commander's joint objectives.

We need to think about how we're going to develop cyberspace operations, and I'm going to specifically look at the officer corps. I've got good visibility in how all the services do this. The Air Force has a leg up in a lot of ways but we haven't gotten there yet. We still have, and I know we're looking at changing this and there's a lot of talk about how we'll do this, but we tend to train communicators or we train intel folks or we train cyber folks or whoever it is, so they spend ten years in that stovepipe.

What I need, if I'm sitting as the J3 of CYBERCOM or I'm a J3 or J5 at a COCOM, I need somebody that understands all aspects of cyberspace operations. I need somebody that after ten years they come in as a major, they've worked in a NOSC. They know how to provide, operate, secure, maintain networks. They've worked in active defense. They know how to do hunt teams and vulnerability analysis and all that. Then they've worked outside of government networks. They know what it's like to be able to go out and do things that are outside our networks that help us achieve our goals, whether that's the ability to kill the archer that's attacking us, or that's the ability to project power in and through cyberspace.

So I need that officer to have experience in all three of those lines of operation, if you will, so they can effectively bring that together to satisfy the Joint Force Commander's objectives.

Then the fourth thing I would tell you, I would suggest that these discussions we have that say is cyber intel? Is cyber com? Is cyber IT? The lexicon is very important and I would argue that the most useful or the most appropriate use of the word

cyber is as part of the compound word cyberspace. And cyberspace is that environment that we create by plugging all that stuff together.

Within that domain or within that environment, then we conduct cyberspace operations.

So if you believe that, then just like operations in air, land, maritime, space, it's supported by intelligence. It's supported by IT. It's supported by com. All of those things are supporting functions to operations in cyberspace. I think that's the most useful way to think of it. Then you can apply all that joint doctrine and all those things we figured out about how to plan and execute operations.

I would say the one nuance of that and what I struggle with a lot to get the operators to grab ahold of this is that when we talk about what does it take to provision cyberspace, we can't fundamentally alter any of the other domains, but cyberspace is a manmade domain. So when we talk about JIE or we talk about any kind of an IT system, that system should be built specifically to satisfy the operational requirement because we can shape cyberspace in the way we can shape no other domain.

The challenge is these operational people up here, they don't want to get into that business. They want to leave that to General Hawkins and people like that. We have to have a relationship between the people that build and secure that domain so that once the domain is created it satisfies the operational concept of operations as opposed to having to alter your concept of operations because you're limited by the way your domain is constructed. So drawing that linkage is extremely important.

In order to do all of that I would assert, and there's a lot of technological gaps, but the three that strike me every day as very significant are number one, a collaborative environment that allows us to tie together all of these teams, all of these headquarters, all of this C2 structure we've put together. For those, it's a largely Air Force crowd obviously, so if you think about TBMCS and what we wanted it to be which is to be able to do that operational planning, distribute it down to the tactical level, establish a collaborative environment that we can do that planning and integration -- but it can't be Share Point and Excel spreadsheets if we're going to do cyberspace operations. So we need that system that allows us to do the collaborative planning and execution globally in a way that at CYBERCOM the J3 can have an understanding of what's going on, that we can allow regional combatant commanders and services to do as much as they can, and then be able to understand when it has global effects or when it has impacts outside of their particular area.

So that collaborative planning and execution system that we need is a huge technological gap.

The second gap that I'm very concerned with is this ability to identify key cyber terrain. This is the sensor to shooter thing. If I take any system, BMDS for example, I've got to have sensors that are over whatever country it is that's going to launch the system, it's got to get the data back to various headquarters. If we decide to launch an interceptor, all that information has got to go to the right place. Look at all of the systems that have to come together to make up that key cyber terrain.

I have to have a way to rapidly technically enumerate that. Then I've got to understand where all the vulnerabilities are. Then I've got to understand the intelligence, understand what the enemy capability intent to take advantage of that vulnerability so that I can guide my forces that do the operations, the active defense and the offense, at those enemy capabilities intent that will have the effect on what my key cyber terrain is at the time.

About a year or so ago the Air Force did that with the RPA enterprise. It took them about a year to articulate all of that. DISA CONUS now monitors that very closely along with AFCYBER so you can figure out that from the time the pilot pulled the stick back in Las Vegas and the elevator moved 1.4 seconds later, what are all the connections to take place. I would argue that as soon as that was done, something significant changed in that environment and it needs to be done again. So the way to rapidly articulate the key cyber terrain at a technical aspect, pair it to the vulnerabilities and the capability intent so we can direct the forces where they need to be is fundamental.

The last thing we need, we struggle every day to understand the impact of things we do in cyberspace. We need the equivalent of JMEMs, the Joint Munitions Effectiveness Manual. What is this thing going to do? If we drop a JDAM on this building somebody can tell you how many windows are going to break, how many people are going to get hurt, how many people are going to get killed. What we struggle with cyberspace is we can't articulate at that same level of fidelity, so the senior commanders the senior policy-makers, none of whom for the most part grew up in this domain, struggle to understand it when we come in and start talking about what we can do and what we can't do.

So our ability to understand what's the PK of delivering the effect we need, and what is the potential for fratricide and collateral damage? It applies just as much if not more in making decisions with what we do in our own cyberspace, right? Because anything I do that hardens the network, does active defense, does

those sorts of things has the potential to reduce my C2 agility, my operational flexibility, all of that. So I have to understand the impact of things I do in my networks as well as the things I do in other networks. And being able to articulate those, understand those, understand the secondary effects in a very tactically and technically complex domain is fundamental to us moving cyberspace operations into where I would argue it needs to be.

Thank you very much, and I'll look forward to your questions.

Moderator: Thank you, gentlemen. We're going to start of talking about people. General Otto in particular talked about the growth in the work force. Several questions came out on that, and basically where do you source the kinds of people that you want to be our cyber warriors for the future? What kind of skill sets do they need and are they out there?

Lt. Gen. Otto: I'll take the first swing at that. I think as a nation we need to really encourage our kids and your grandkids to get into STEM fields. We as an Air Force have spent a lot of time and attention telling our airmen to get a degree. I think that was a wonderful and necessary first step. Now we need to encourage let's get STEM degrees. What we see time in and time out, as I go throughout the enterprise and I run into airmen that are doing exquisite work in cyber, and I'm Big A Airman -- civilian, enlisted, officer -- and I find out what's their background? It tends to relate back to technical fields. I'm an electrical engineer; I'm a physicist; I'm a computer science engineer. Those are the kind of skill sets that are really doing the high end stuff, but when you talk to the people doing some of the nug work, it would be people that -- the people who are really doing the heroic work, people that were not required to have any degree, and you find out oh, I had two years of college before I came into the Air Force and it was, I was a math major. So what you find is a string that you can pull throughout that leads us to saying it is more technical than philosophical. So gearing up a work force to do that is something that we need to do.

Within the intelligence, surveillance, reconnaissance world, where we seem to have one of our biggest shortages is in our all-source analysts, but we have a plan to take care of that. There's certainly some testing that we can do that we have adopted. Historically what we've done is we've taken airmen after their first assignment and we've said hey, based on what we see in you, you have a great ability to absorb the kind of information that would make you a success in cyber. So let's vector you that way.

Now we can't meet all the requirements that way, so we're looking at doing some testing of airmen to find out do they have the skill sets that translate. The testing seems too early to tell but it seems to be promising, and then what we'll do is go back after they've been in the field for a while and find out what's the washout rate of the people that were first accessions and taken into cyber versus those that we took after the first assignment.

Lt. Gen. Basla: Let me give you a little bit of context of where we are today.

Today we have a level that our airmen must meet when they take the basic entrance test to come into the Air Force. WE have that as a high level. But that's not enough of a filter to determine who's going to be successful in the cyberspace areas. As General Williams said, there are many areas that are associated with cyberspace. So we're looking at ways to raise that bar.

We have developed an aptitude test like General Otto said. The jury's still out on how well we are doing with that.

The fact of the matter is, most of our airmen on the keyboard are going to be our enlisted folks from the mission teams that Cyber Command has asked us for, with the officers leading that group as General Williams said. So we've got to develop those folks over a period of time to meet their specific mission needs.

Do we have enough? Probably not today based on what we forecast for the demand of tomorrow. Very good anecdotal information from the United States Air Force Academy. Some of you know that those that attend the Academy can list the career fields that they'd like to go in upon graduation, and by order of merit they're awarded those career fields based on requirements.

In the past the communications career field, the one I grew up in, was not one of their top choices, so many of them were put into communications as non-volunteers. Not all, but some. The fact of the matter is most recently as we've now developed a cyberspace career field of which folks that come from my background have some propensity to support, there are more Academy cadets that are interested in going into that kind of career field, with the technical degrees that General Otto talked about.

So I think that do we have enough? No. Do we have some sights in mind that forecast that we've got people interested? Yes. Do we have to emphasize STEM? Absolutely. Once we get these people into the right career fields, how are going to keep them?

We're looking across the Department of Defense for standard terms of enlistment. We're looking across the Department of Defense for standard bonuses. So that an airman sitting next to a sailor sitting next to a soldier sitting next to a marine has the same kind of compensation.

Just like General Otto said, in Big A, this is total force. This is all components of the Air Force and the civilians and our contract award force. We are now going through an exercise looking at the composition of the Air Force contribution to the U.S. Cyber Command requirements.

So a big job in front of us with a lot of attention placed on this right now.

Moderator: Another people-related question here directed primarily to General Williams, but address the role of civilians and contractors in offensive cyber operations given the restrictions of the laws of armed conflict.

Maj. Gen. Williams: Next question? [Laughter].

I would say if I took that up one level that everything that we do outside of U.S. government networks is subject to all the laws of armed conflict, it's limited by policy, authorities, rules of engagement. All of the things that we do in cyberspace outside our space, in other words, are limited by all the things we do in the physical domains outside of our space. So there are very specific rules, criteria, law that dictate what contractors can do and what civilians can do. We comply with all of those across all of the lines of operation with cyberspace.

I guess what I would throw on there at the end is we're getting to really the issue of authorities. There are a lot of authorities involved with cyberspace operations and those authorities guide who can do what. A lot of the authorities we arm wrestle over are those authorities that involve intelligence oversight and privacy and all of those things which we absolutely ensure compliance with.

There's a whole other set of authorities about who can operate on this system based on who the CIO and the DAA and the program manager and all of that.

So this issue of authorities, the understanding of who can do what where, when, is all very complex when you get outside of the individual stovepipe of whatever it is, which gets back to this thought of key cyber terrain. We've got a lot of people that work in the stovepipes. We need more people that work across all of those stovepipes and understand what that is.

But the bottom line out of that is the rules are established on the correct role for military, civilian and contractors and like everything, my theme if you will, is we can apply all of those and to apply those to cyberspace operations.

Moderator: This is directed to any of you, all of you. Given resource constraints both in money and manpower, is there any thought of collectively bringing A2 and A6 together to reduce those issues? There were actually two questions on this. One of them points out that the Navy apparently has made that move already.

Lt. Gen. Basla: Can I start that?

I'll say that based on the Strategic Choices Management Review that the Secretary of Defense kicked off some time ago and the results of that SCMR, the Chief of Staff of the Air Force has directed a look at our Headquarters Air Force organization as well as the MAJCOMs out there. So we're starting at the headquarters level.

The Chief and the Acting Secretary have said nothing is off the table. One potential reorganization opportunity is the combination of the 2 and the 6 as the questioner suggested, but that is one potential.

Let me tell you what my position is on that. The Air Force management headquarter has a target of reducing 20 percent. That's kind of what the SCMR has asked us to do and our Chief said and our Secretary said we will achieve.

I think cyberspace, as I kind of indicted in my opening remarks, supports all the warfighting domains, all the support activities, all the mission areas in our Air Force. Including the personnel, including the medical, including the logistics, including what's traditionally known as operations, intelligence, et cetera. I'm not going to speak for General Otto but I've gotten an idea what his focus areas are.

A combination of A2/A6 may refocus the attention of what the 6 has to do -- support all mission areas -- and focus on just a portion of those mission areas. I've got some concerns about that. It doesn't mean it won't work, but I have some concerns about that. We must look at the fabric supporting all the mission areas from an IT perspective and a cyberspace perspective. So we are looking at all the opportunities, that being one of them.

Lt. Gen. Otto: I think Mike addresses that one pretty well.

Just philosophically, when the Navy went to an N2/N6 which they have done and it has been effective for them, the thing that drove them to that was a mission effect they were trying to achieve, not necessarily where we are today which is trying to achieve budgetary and personnel reductions.

There are clearly some very good reasons why we would combine the 2 and the 6. There are also some reasons, and Mike touched on some, why that might sub-optimize various aspects of either the 6 or the 2.

At the end of the day my approach to organizational constructs is there are positives and negatives to various organizational constructs and we're going to have to just lay those out and see what were we trying to achieve, and then with this construct does that get us there, or are there other approaches that will also have positive and negatives, and which is the best way to go. Napoleon laid out the structure we've got today back in 1803 or something. It's worked pretty well. But we have over time and in various organizations, and you see different combinations in various combatant commands and within the Air Force, and so what it points out is that different regions may also have different rationale for going one way or the other based upon the challenges that they face.

The Air Force faces some really extreme challenges right now and we have to look at everything and this is one that we are looking at very closely, but the jury's still out.

Moderator: This one's directed to General Williams, but any of you can answer this. Certainly the sequestration has been on everybody's mind. IT's very obvious to everybody when you ground a fighter squadron what the impacts are. What kind of impacts, if any, have sequestration affected in the cyber operations areas? Are we any less safe? Any major consequences of the sequester?

Maj. Gen. Williams: Luckily Brigadier General Linda Meddler is here as our J8 and I'll turn that question over to her.

I would just say two quick things. In the macro perspective, we are just now defining what readiness is for cyberspace operations forces. Because just like we struggle frankly to adequately define readiness with all the other forces through things like [SORTS] and [DERS] for those of you familiar with that, to first define what readiness is and then to be able to link the dollars to readiness, right? A lot of people think they know why we're not ready, we need more flying hours, we need more this, we need more that. And when you really do the analytics to say where

should my next dollar go to raise my overall level of readiness, is it a personnel issue, is it an equipment issue, is it a capability issue, is it a training issue, is it a range issue? We have all of those same considerations with cyberspace operations. So we are working through defining what does readiness mean and how do each of those play there? Then as long as I'm Cyber Command, after my experience working readiness in the Air Force, I'm going to insist as much as I can on some rigor to linking dollars to readiness so we can articulate that up the chain.

More specifically to your question, give me some of that cyber stuff, everybody wants cyber stuff. So we have actually been the benefit of probably less cuts than maybe some other fields have been out there. So right now we're trying to take advantage of that. As we grow as a sub-unified command and we start plugging into the FCB, JSIDS, JROC process we will continue to mature and better define our requirements. But right now I'd say that we have been the benefit of probably less impact in certain ways However particularly O&M dollars, MilCon, all those sorts of things are certainly an impact on Cyber Command like they are everywhere else.

Moderator: We're just about out of time. I want to give each of you a few moments, if you'd like, for some closing comments, if any of our discussion has jarred your memory on something you wanted to say.

Lt. Gen. Basla: Thanks Scott.

I would say again than you all for participating. As General Williams said, this is a very important growing capability in our nation's defense portfolio.

Industry has a large role in this. Industry can help us get at that problem that we just talked about. Lots of pressure on dollars but lots of rising requirements out there.

We need to find ways that we can automate some of the manpower intensive capabilities that we currently are responsible for in the cyberspace domain so that we can apply those available resources to the absolutely most essential mission areas.

I do appreciate all the men and women, including our civilians and our contractors, that are supporting this important mission area. So thanks very much AFA for letting me participate.

Lt. Gen. Otto: The only thing I want to add that I didn't talk about before is this is, when we talk about cyberspace as a manmade domain, this is a big data problem on steroids. When you

look at the amount of information that is transmitted every day across all of the computers, probably 90 percent of the people in here have Facebook accounts, there are over a billion Facebook holders around the world, they transmit more data in a day than any book ever printed in a day. So you think about the magnitude of that problem in terms of either protecting what we want to protect in the United States or being able to impact elsewhere, and then making sense of the data that's flowing, it's a huge problem and it is going to take a tremendous amount of investment, a tremendous amount of thought. We aren't going to get it right all the time. So we're going to have to work our way through the many problems that we face.

I'm just thankful that our nation has the attention that it's getting right now, because we're late, but better late than never.

Maj. Gen. Williams: I'd just like to emphasize the importance of our partnership with industry. If you look at those three technical challenges I articulated, all of those are essentially, let's call them IT solutions. Right? Our record of developing IT solutions that ultimately satisfy the operational requirements is not always that great. Right? And the acquisition process to build a ship, a plane or a tank is maybe not the one that we need to create an IT solution. I would argue the fundamental failure is we have an operational requirement -- could be a medical logistician, could be me. It's got to be translated into requirement speak and engineers, have got to understand what it is. Then you've got to have the acquisition strategy lines up to support all of that.

How often do we have a person that understands whether all three of those are really moving in the right direction? They're going to deliver the solution at the end? We end up parsing these out to different areas and at the end of the day we frequently don't get exactly what we need.

So I think our ability to partner with industry and link all three of those lines of operation, if you will, on the acquisition side is fundamental and is extremely important.

Again, I'd like to echo what the other panel members said, and thank you very much to AFA for the opportunity today. We appreciate the work that all of you do to support cyberspace operations. It is a direct contributor to national security and it is important. So thank you very much.

# # # #