

Major General Richard E. Webber, Commander
24th Air Force

LA Symposium

19 November 2009

MajGen Webber: Thank you very much, Sandy, for the kind introduction. You read it exactly the way we wrote it, right? [Laughter]. And congratulations to our Outstanding Airmen. If any of you have any cyber skills, we'll be talking to you later.

Welcome to everybody. What an exciting mission to be doing the first of pulling this mission area together. [...Take Skip...] it's equally complex and extremely difficult to move ahead in this arena, and I'm going to lay out our challenges.

Next slide.

What I'm going to show today is a combination of a Cyber 101 discussion that I had with our component Numbered Air Force Commanders, our warfighters, to kind of lay out initially our perceptions of how we see the landscape of this domain. Then I'm going to lay in on top of that big chunks of the briefings that I gave to my joint commanders when I laid out our presentation of Air Force forces, and then kind of tell you what's on the horizon for the industry folks so you can be seeing the challenges as we see that.

Next slide.

Some bottom lines up front.

There's a lot of discussion about whether or not this domain, this operational domain is manmade. I think you can argue on equal sides of this. But when you describe this in terms of we're the ones who put that network together, we're the ones who put out that hardware and that software, and every time we push a patch we change that environment, change that domain. That is what I'm talking about when I say this is a manmade operational domain. It's a place. It's a physical domain. It's not a mission by itself. Many times we will try to lose our way and call this a mission. This is a place.

This is a place where operations are conducted. Like land, sea, air and space missions, and our job here is to integrate these missions -- not integrate the domains -- integrate the missions in support of joint warfighters.

Last, it's about mission assurance. It's about assuring our ability to get that joint mission down. It's not about assuring the network.

I will never forget in my first experience in this environment, and I think Dave Warner would pile on here. I was the CIO for Air Force Space Command. We had a pretty significant hacking attack going on against the Peterson Air Force Base complex. The recommendation, and this was quite some time ago, was to what? What did we used to do? Disconnect. We create our own denial of service by disconnecting. We need to learn to fight through, to fight through an attack. So it's about mission assurance.

I know this will be a long road because we are really making a culture change in this concept of fighting through an attack, but all it takes is one step and those combatant commanders, those operators are going to say I knew that, they didn't mean it. So this is going to be tough and we all need to work this together.

Next slide.

This is the Joint Pub 1 definition of cyber space. Read it. What does it say? Interdependent networks. Technology infrastructures. Internet. Telecommunication networks. Computers. Embedded processors. That's the universe right there. That is absolutely huge. I know there's still some debate going on about the joint definition of information operations and how it all fits together, but suffice it to say that we're going to focus like a laser beam on operating and defending our Air Force networks.

Next slide.

Domain relationships I think are important to kind of get a starting point of how to view this domain. We all know how much of the earth and the land and the sea, what percentages cover the earth's surface. And how we argued as a new Air Force about the atmosphere around that, covering the globe completely. Then as we shift from the air to space, from Bernoulli to Kepler's laws and the infinity of space and beyond. Cyber covers the entire spectrum of conflict. It's even less feasible that you could conduct an operation without access to cyber than to try to do it without access to sea or land or air. Very very difficult domain to work in.

Next slide.

So what I did was I tried to take some domain similarities and differences in my 101 discussion with our combatant commanders in the Air Force, and to kind of shape and structure, and I'm sure some of these will come back in the question and answer period.

Cyber space is not really the key to our asymmetric advantage. It's our movement of information, which we do with and through cyber space. That's what makes us so dominant on the battlefield. Any time you have an asymmetric advantage you have created a potential Achilles heel. A way for somebody to come at you from a different angle.

If you look at what it would take for another nation to create a near peer capability against us in space or in the air or at sea or on land, you would say that's a pretty stiff price, extremely stiff price to enter, but we're in a world in the cyber domain where the price of entry is extremely low. A 13 year old with a laptop, a terrorist, a small non-government organization, third world nations, individuals. Much different price of entry.

The defense industrial base really is required for all domains, and we have our own here but you're going to see that, we've read this, all of us, that cyber space has been used against all of our domains to exfiltrate information from our civilian sector and make other nations more competitive with us. Very low cost of entry, and when you can get in with a low cost of entry and it's a way to angle against an asymmetric advantage, very attractive.

Next slide.

The pace of change is going to be a complexity you face in all domains, but it's particularly rapid in cyber. Very interestingly, it's not pushed by the military. It's pushed by the civilian sector. And if I'm looking for a new defensive tool, I'm going to need that sometime in hours or days. That's quite a challenging acquisition cycle.

We're still working on defining in this domain what sovereignty means or what attribution means. If an enemy attacks a United States Navy aircraft carrier in the middle of the ocean, that's a very clear attack on the United States. If a very important communication satellite is attacked, not as clear, but I think we all have in our mind exactly what that means. When that happens in cyber, it's very difficult to attribute where that attack came from. At every fork in the road in the design of the internet, at every fork in the road we took consciously the anonymous path. We took the anonymous path. So attribution is much less clear and we've got a lot of work to do on our policies and our doctrine in this domain.

Next slide.

We have decades of experience fighting through an attack in land, sea and air. We talk about offensive and defensive counter-air. We work our way through that all the time. But cyber space is primarily in the civil sector and we have to work

a mind shift that I think is very similar to the mind shift that General James described in the space world. When he's working with a satellite and all of a sudden part of it doesn't work or he can't even talk to the satellite, decades ago we would say well, let's just shift from the A side to the B side. There wasn't this thought that maybe somebody's messing with your system. We need to rule that out first. So that's that shift in mind set here that am I under attack? Let's rule that out first. Then how do you fight your way through that attack so that you can support that mission even while you're fighting to keep that network operational in support of that mission.

Next slide.

This is the 24th Air Force mission. Establish and extend the networks, operate and defend those, and provide when directed capabilities in, through and from. And just like you heard from General James, look at number one on my mission essential task list there. Create an awareness of my battle space. That is really job one. Then obviously develop the command and control that goes with that.

Next slide.

Here's how I view the joint relationships that we're going to need. First of all, General Kehler and Air Force Space Command have been designated as the lead MAJCOM for this mission area, so they are responsible for the organize, train and equip responsibilities in this arena.

They also will have other things like the operational readiness reporting as well as the DAA responsibilities. So that 24th Air Force can focus like a laser beam on operations. We in fact don't even have any installations where we are the host. We are a tenant on all of our bases. So we are focused on operations.

Now we do have a little bit of an anomaly with our combat com forces. They still are presented by Air Combat Command to Joint Forces Command. Obviously that relationship, I would prefer to have it through and including 24th Air Force and we're working on that. But we do need to work, and it's already in process, a memorandum of agreement. I call this kind of the lead sled dog approach between Air Force Space Command and Air Combat Command. For decades they have done an outstanding job of resourcing this entire mission area and we're in the process of transferring that over to Air Force Space Command.

Right now wherever you have the center of mass, whether it's in the communications world or the logistics world or you're talking combat com, wherever that center of mass is they ought to be the lead sled dog, but it all needs to fairly quickly transfer

over to Air Force Space Command, and we're in the process of doing that.

Next slide.

In my presentation to my joint bosses, we talked about three touch points of where we need to work, how we relate with our joint commanders.

The first is what I call an Ace Light. It's our air component coordination element. This is a term that the Air Force uses to attach to joint commanders. And what I would like here is collocated with U.S. Cyber Command when it does stand up, I want to have a permanent, 24x7 face from the air component located at Fort Meade with the Commander of U.S. Cyber Com.

So what I'm thinking about here is eventually a one star colonel, maybe two or three action officers, to be our 24x7 presence.

Now in the mean time, since we don't have that extra general officer, it's going to be me and my vice commander, Charlie Shugg, doing a lot of road time back and forth. But as soon as that stands up, we will be there. We've already picked who will be our colonel to go into that position.

Now U.S. Cyber Com has already decided that they will have a liaison to each of the key combatant commands. They've already gone to the services and asked for six colonels. Three of those colonels are going to be Air Force colonels. They've already been selected to be the liaison officers. And my thoughts there are that if they do synchronization of forces at that engaged combatant command then we are going to offer folks who are familiar with how the Air Force systems operate and are there to make sure that we don't have any synchronization issues with our forces in the rear.

Then last, is a relationship that I need to establish with the component numbered air forces, with those coalition commanders for our air components.

We were very careful of our choice of words here and chose a term that I think is very descriptive of the fact that we are never in the Air Force going to have the preponderance of forces in this arena, so unlike Air Mobility, unlike Space, we didn't use a term like DIRMOB4 or DIRSPACE4, we used something that we borrowed from the Special Ops community where they have a Special Ops liaison element. So we're going to call this entity a Cyber Operations Liaison Element. This will be how we feed back and forth the commander's intent, work out what they think is most important to be defended, their defended asset list. This will be where we do synchronization. And if they've got a special

operation coming up in the next 24 or 48 or 72 hours, this is where we will flow that back and forth. I think in many cases this entity could be a cell located on our 624th Ops Center. Obviously in time of war you may want to move forward. But it all matters in my mind, where do you do synchronization of forces?

Next slide.

This is our presentation of capabilities. I cannot lay it out by squadron because that starts to make it classified. In the upper left hand side is the operational integration that General James was talking about where if you look at this domain of space and then this domain of cyber, there's clearly an overlap area. I don't know how big that is, but there's clearly a synergy there that the Air Force forces bring to the joint fight.

So we will work that operational integration between our ops centers. Then you see that the 67th Net Warfare Wing are the folks that give us our full spectrum operations on the network.

The 688th is the old Air Force Information Operations Center, mostly. They will do our tactics, techniques, procedures. They will be the folks that develop the new tools, do a quick checkout of the tools. They also do the Blue Team assessment where we'll roll into some Air Force entity and identify any potential weaknesses that they might have. As well as the hunter teams. These would be folks that would defend key parts of our Air Force enterprise.

The 689th is our Combat Com warriors, and they do the rapid get out of town, set up communications anywhere around the globe. Then we will also have, like every other component numbered air force has in the Air Force, a dedicated intelligence, surveillance and reconnaissance agency group, and it's been stood up as the 770th. It's provisional. That number will change when it gets formally approved. That will do our signals intelligence support, our threat analysis, as well as warning and target development. So that is kind of the presentation of our capabilities.

Next slide.

Next I'd like to kind of turn our attention towards what do you mean by mission assurance, and maybe draw some pictures in your mind of how one might go about doing that.

Today I would argue that our defenses are very much like the Maginot Line. We're probably at the point where building the wall higher and higher is not going to be effective for us. We need a layered defense. A defense in depth.

So what our vision here is is if we work with those backbone providers, and since I see quite a few blue suiters out there, what happens every time you fire up your computer? You click on this box that says what? It's very very definitive about what you can use that computer for, what you can't use that computer for. So because of that we can go to our backbone providers, as an example, and say if you see this signature of this malware or this virus and it's going towards one of my gates, why don't you just put it into a black hole? Then I combine that forward entity in the cloud with the gateways that I have where I have sensors and can do some defenses there, with, and this is another addition, a hard look at that defended asset list. This is where you'd go to perhaps a functional area like the medical world or the personnel world and you say what hardware, what software is mission essential? Or you go to a regional Air Operation Center or a functional Ops Center like Space or Mobility. That's where you look at how can I make sure that we assure this mission? How do I defend in depth? Where are my redundancies? Where do I focus sensors? How do I defend this in order to make sure that under attack we can fight our way through the attack? So that's deliberate planning.

Next slide.

When you get into crisis action, this would be X hours out, maybe days or weeks, where the joint commander wants to plan a combat operation. Now I'm getting into crisis action planning.

Let's say this is a Special Ops rescue mission to rescue Jessica Lynch. Hypothetically. You look at that layout of what that commander wants to do and you say what pieces of this are critical to the execution of that mission? He says well, I've got to have eyes on, I've got to have that Predator or Reaper, I've got to have those tactical ground controllers, I've got to be able to be lashing up my command centers. You look at that and say okay, these are the pieces that we need.

Next slide.

Then you go in there and you say well, if that Predator or Reaper is mission essential, you need some backups here, so perhaps you get a dedicated hot backup on the satellite link. You may look at that Army circuit and say I need some duplication there. Then you would also go to the intelligence community and say hey, are you seeing anything that could be a potential threat to this operation in the network realm?

Next slide.

Then when you get into the actual operation, perhaps I could take my very limited sensor capabilities which look at a small portion of the entire network on any given day, and I could shift

those resources, reallocate them, to look very closely at these systems that are mission essential to getting this mission done. Then with that additional situational awareness, this is where I could put my hunter teams to defend if I find myself under attack. That would be how we fight through the attack. Switching to backups, switching to alternate modes, and actually trying to block and defend against that attack. That's fighting through the attack. An entirely new construct.

Next slide.

Looking to the future, these are kind of the near term close-in alligators that we're looking at right now. We need to normalize how we operate and how we defend this enterprise. And I definitely think it's going to be a crawl, walk and run, because it was set up as a communications centric enterprise, and now we have to think about this as a weapon system, as something that we have to fight through an attack. And we are under attack literally every day.

We need to operationalize our command and control. When we look back at our recent lessons learned with various malware, we find a system that was bypassing, was going down communications signals. Many times it was bypassing commanders at all levels with the direction. It was coming from multiple sources. We need to tighten up all of those things. And just like we fly and fight on the air, land and sea.

We need to mature our joint relationships. This is not just the relationship with U.S. Cyber Command and U.S. Strategic Command, but also with my fellow component numbered air forces and how they support their joint commanders around the globe.

We need to partner with industry. I look here at two different things. One is the major providers that support our enterprise. And if the Air Force has an enterprise of about half a million unclassified computers, with that you get normally certain enterprise relationships that you negotiate with your providers. So whether that is a backbone provider like the folks that do the long haul communications or it's the operating system individuals or anti-virus, or the people who build servers and routers, each of those folks can, I think, provide us information that would classically be kind of intelligence in nature of what's going on out in the environment that we're operating. And if we properly use that, that will help us build an awareness of what's going on.

Total force integration. In these times we are not going to grow the Air Force. So most of our growth in this area I expect to be in either the Guard or the Reserve. I have a very exciting presentation from our Guard folks who are already talking about aligning a combat communications wing with the 689th Combat Com

Wing. They want to align an information, a Guard information operations wing with the 688th Information Operations Wing. And then two groups aligned with the 67th Net Warfare Wing. So very very exciting times.

Then last, but I'm going to go back up and talk about the Ops Center last, but last on this list is building a component numbered air force staff. When I departed for this trip of 200 authorized we have 40 bright and shiny faces present for duty. Those are being augmented by anywhere from 20 to 30 additional folks provided by General Kehler that are there on temporary duty or Guard or Reserve folks coming in to help us out.

Just like General Klotz talked about, you can look at these folks in the face and they are excited. They are doing something that's never been done before. But you also think in the back of your mind as you're dealing with the complexities of this mission area, they're going to look back, and yes, your picture is the first one on the left, but they're going to look back and they're going to say what were those folks thinking? What were they thinking? And they are peddling as hard as they can to put our arms around a very complex mission and really change a focus towards supporting our warfighters.

Then to go back to the command center. Our command center is very communications/op center centric. As you might expect. That's where its roots are from. We have a limited ability to monitor various pipes. We find it difficult to tie those pipes to a specific mission impact if I lose that circuit. And we have the ability to push patches. But it is not a warfighting strategy to task organization.

So as we move that organization from Barksdale to Kelly Field in San Antonio, we're changing, this is the equivalent if you're flying your F-15 and you decide while we're flying we're going to change out one of the engines and then, and sir, you might like this, let's change out the OFP, the operational flight program at the same time, and we will not crash. We will not crash. WE cannot crash. So right now we are already remotely operating the Barksdale infrastructure from San Antonio. Very shortly we'll have all the hardware and operations going on in San Antonio. And by the end of the year we will have the very beginning of a strategy to task in our operations center. But it's definitely going to be crawl, walk and run.

That concludes my remarks and I look forward to any questions that you might have.

[Applause].

Moderator: Clearly no lack of interest, I must say.

General Webber, there are many agencies, departments involved in the cyber business, federal departments, other than the Department of Defense, Army, Navy, perhaps DoD agencies, and even international organizations. So how do you see a coordination effort in terms of warfighting?

MajGen Webber: Let me break that into a few pieces.

First of all, we need to work completely integrated with the intelligence community. We cannot do our mission without them. That is why in many places around the globe, that's why we are colocated with the intelligence agencies. So this mission is inherently interagency from the very beginning.

It's also, if I'm working with the continental United States I also will have to be teaming with law enforcement agencies. So we need to have all of those interagency relationships in place.

Unlike other warfighting domains, I view this as the combat effect that we create is going to be created at the U.S. CyberCom level, and all the services will bring important capabilities to the table that will be combined with law enforcement and intelligence and other agencies' capabilities. But really, you will be creating that effect at the U.S. CyberCom level.

It will also be coalition. We already have within the 688th Information Operations Wing, we already have two liaison officers from other nations and we're going to use those as our jump start. But not only do I need liaison officers, we're also looking at can we get exchange officers. Young folks, captains, majors that perhaps could work in our ops center. So we're going both the exchange route and the liaison officer route.

Moderator: We have a number of questions regarding career fields. This is an interesting one because there are those who as we look at cyber and we learn more about the kind of capabilities that are needed among the work force, some talk about cyber professionals coming from the intelligence community, others from the communications area. Can you give us some thoughts on that? And where do you think the next folks will come from? Will it require training from the very first, for the second lieutenant, from the enlisted level, right down at the beginning? Or will we be growing them from different career fields?

MajGen Webber: Did those come from the Outstanding Airmen? [Laughter].

Interesting question. Early on in my job I went to a classified location to talk to one of my units and as you might expect in this area, all first term airmen or first lieutenants or second lieutenants. I said before you say anything, before you

give me a mission briefing, let's go around the table and around the room and you tell me where you came from and how you got to this place in your career. It kind of broke down into five equal parts. This is kind of a totally subjective thing, but it was really illuminating to me about this mission area. About one-fifth were from the communications world, no surprise there. About one-fifth were from intelligence, no surprise there. For the officers, about one-fifth were engineers. And it wasn't always computer science. It was different kinds of engineering. About one-fifth were from acquisition. And then the biggest surprise to me was this last one-fifth that was from all other walks of life. Airmen who were great, had great computer skills, but they might be in security police or services or civil engineering. They came from all walks of life. We had somehow found out about their talents and by name requested them and they had passed tests and we were training them.

So if there's a message I could leave about how do you develop this, and this is the issue that General Kehler will be addressing as we look at how do you develop Airmen for this career field, and I think he starts to think about creating a combat capability in a domain. That means you need all walks of life. Very similar to his space professional concept, is perhaps we need a cyber professional concept.

I know recently we have done a major reorganization of our specialties and our training in the communications world, but when that person comes out of the communications world I still need to make sure that they have training in signals intelligence. If that person starts off at Sheppard and comes out as a trained signals intelligence expert, do they have all the computer skills that they need? Or even if they come out with an engineering degree, do they know at the fundamental level how a computer network operates?

So we're going to have to put together all the pieces. And it's not just the initial training. It's developing a combat capability. Because I think it's very real to expect that an Airman, officer or enlisted, is going to probably have a minimum of two courses as we understand it now before they are going to show up at their unit. Then they're going to have a period of apprenticeship to get them up to a combat ready level.

Now if that period of training and apprenticeship and then maybe later on a couple more courses to round them out. If that initial training takes 18 to 24 months, I can't afford to lose that Airman 12 months later. So we're going to need a period of payback after they're combat ready. So let's say you need at least 24 months of payback.

Then with all the classes, and typically by the time they're in that first tour, apprenticeship and all that training. Let's

say they went to four different classes, can you afford to have that Airman go somewhere else in the Air Force? I think initially for the young folks you're going to probably want to have at least two back-to-back assignments. So if they start off in the intelligence world, they could flow over into the 67th or the 688th, or if they started off with us on the 24th side, then they could flow into the intelligence community.

So we're going to have to look at how you grow this capability in the entire career field.

Moderator: You heard General James today talk about jamming as one of his major concerns. You mentioned on the slide how you would go out to folks and ask them what was the most important thing they needed. So who's responsible for spectrum control?

MajGen Webber: Spectrum control comes under the AFFMA, Air Force Frequency Management Agency which is assigned under General Kehler. Those are the folks that do it internationally and nationally.

Moderator: And you would coordinate from them for that kind of activity?

MajGen Webber: If I needed frequency spectrum, that's where I would go.

Moderator: You mentioned also in this realm, cyber, where we may have near peer competitors really, only one, only place, low cost, to enter from an aggressor, fighting through the attack. Do you have a level of confidence that the DoD budgeteers and the Congress has the same sense of the kind of resources and will supply those? And do you know what the resources you need are?

MajGen Webber: I think this is going to be a crawl, walk, run mission area. As we put our arms around it historically, we viewed this from our communications stovepipes or our intelligence stovepipes and now we're bringing it all together for the first time.

I almost feel like it's the early days of flight with the Wright Brothers. First of all you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time and it's going to be growing. But clearly we're not as big as the air part of the Air Force or the space part of the Air Force, but we're growing.

Moderator: We have so many questions, we've got to bring this to a close, but I'm going to give out shortly your personal

phone number and room number and give them the opportunity --
[Laughter].

General Webber, thank you very much for the informative presentation and being with us today.

MajGen Webber: Thank you very much.

#