

## Forum on Cyberspace

Lieutenant General Robert J. Elder, Jr.  
Commander, 8<sup>th</sup> Air Force, Air Combat Command

25 September 2007

**Moderator:** -- Combatant Commander for Global Air Strike and Integration, and the Commander, Bomber and Reconnaissance Task Force 204. Among those responsibilities, he's leading the way in the establishment of the new Cyber Command. I'll now turn the podium over to Lieutenant General Robert Elder. General Elder.

**LtGen Elder:** Thank you.

I was talking to General Mike Dunn, and originally the slide said "Presentation for Air Force Association, Air, Space and Cyber Conference," next year. Seriously. [Laughter] Mission of the United States Air Force, fly and fight in air space and cyberspace. Next year I'm sure this will be an air space and cyberspace conference.

I want to give you some time for questions. I'm going to try to go through some things relatively quickly and then we can go back and answer those things that perhaps you have more interest in.

It's kind of interesting, this little statement here, this doctrine. This is not the United States doctrine, although it's close to what our doctrine is. This doctrine comes from our good friends in China, not always the ones who are exactly on our side.

The other thing is you're familiar with what happened in Estonia recently, and this is a quote out of *The Economist*, and no, we didn't spell "organize" incorrectly; that's how's the Brits spell it. [Laughter] But that was the statement. And it's interesting, if you don't think about the fact that that's about Estonia and you read that and it had be done with say a maritime blockade or something, you would have thought this was an act of war, and that's really kind of the point. Kind of the situation that we're faced with here is that we do have some peer competitors and we do have some nation-state capabilities that can be organized either officially or unofficially, that can really have a serious impact on how a nation operates, as we saw in Estonia.

This is just a quick overview of what I'm going to try to talk about today. I know there's a lot of questions about the provisional command, so I will hit on that, but I'll talk about the tasking that the Chief and Secretary gave us back in November. I'm also going to try to put in some context. But I think most importantly, what I'd like you to take away from here

now is that this is not something we're going to do next year or the year after; it's the things that we're doing now, and we're continuing to develop our capabilities as we go along.

First of all though, I'd like to set a foundation for this because some people that we talk to think that the Air Force came up with this on our own. I guess I'd like to take credit for having thought of all this and being the hard charger. There's a lot of things we have come up with, but in reality this is all founded in the national guidance. As you see here, this is some things that came out of first the QDR, the Quadrennial Defense Review, that has really talked about the fact that we now have, we're worried about the strategic commons, and one of these strategic commons of great concern to us was space, and the other one was cyberspace. And cyberspace is this area that the QDR said we needed to pay more attention to.

The next set of bullets that you see relates to a thing called the National Military Strategy for Cyberspace Operations, and a lot of people are now looking at this. When it first came out it was considered very revolutionary. Some people are actually trying to back away from it, but the reality is this is the foundation for what you see us doing in the Air Force.

A couple of key points I just want to foot stomp, and I'm going to say this. If you leave here and I haven't made this point that cyberspace is a war-fighting domain, then I haven't, that's one of the key points of this whole discussion. What this national military strategy says is that we must, from a military standpoint for sure, have superiority in cyberspace to be able to do any kind of other military operation.

The next point I put there for some of my friends that like to back away from this and say, well, we have joint doctrine that says this or we have this other doctrine that says this. This particular document said, in a little more detail on that third point, which is that what's been happening in the cyber domain, what's been happening in terms of what you look at in information operations and other command and control has been evolving rapidly, and there's a recognition now that this is not just an enabler. It's not just a C4ISR enabler, it really is an area that we warfight. It is a warfighting domain. Therefore, what it says is that we really need to look at what's in this National Military Strategy for Cyberspace Ops and take this seriously and think about it as the way we're going to things, and it probably will lead to some changes in joint doctrine and the way we do other things.

The last is that this is not a stovepipe, so we're not looking at some of the other capabilities you've heard of before where we're just looking for capabilities in, say information

operations or in intel or something related to this, or C2. It's really all about how we integrate this together.

So this is not the Air Force, this out of the National Military Strategy for Cyberspace Operations; however, the Air Force, everything you see there, that's what we do. So you remember this mission statement that came out shortly after this National Military Strategy for Cyberspace Ops talks about the sovereign options and the need to have the sovereign options. It says we're going to fly and fight in air, space and cyberspace. And we're going to talk a little bit about how we do that.

This framework here, which I'm not going to go through point by point, I want to talk in the generalities, also came out of the National Military Strategy for Cyberspace Ops. But it helps you to frame what we're talking about with cyberspace operations. If you'll look on the top left there, you see that it is not just network operations.

It is not just information operations. As a matter of fact, it says that there are kinetic operations involved. Later on in the presentation, I'll talk about what those are.

It says that there is a law enforcement piece of this, and we're going to show you that a lot of what we're doing relates to how we interact with law enforcement because when we first have an attack we don't know who attacked us. Depending on who the attack is from, it might not be the Department of Defense's job to deal with that. When that happens you have to pass it off. Conversely, in our relationships with law enforcement when they find out that it's not a law enforcement action, this a Department of Defense action, then it comes over to us. So we have that relationship.

Of course the counterintelligence part, while we're not involved in intelligence ourselves, we are interested in people stealing our information. Therefore the counterintelligence piece is important.

The enablers that you see there could be the enablers for any other type of operation in any other domain. I think that's one of the interesting things that helps you understand that this really is a warfighting domain because some of the things that you would look at are exactly the same as you would do if this was a land or air/space domain. And then you look at these joint capability areas that are specified, just take a quick gander at them, you'll say this does not look that much different than what we do in a traditional physical domain.

So the point of all this is, when you take a look at what's in the National Military Strategy for Cyberspace Operations we have a firm foundation for what we're doing in the Air Force, and

we're not being real avant-garde. We are actually trying to lead the implementation of what the national authorities have asked us to do.

I'm just going to get my next slide up here.

This is a quick summary of why are we doing all this. It's shown here, a couple of foot stompers. The way the Air Force operates with this idea of centralized control and decentralized execution, that's what gives us this speed, range, and flexibility. At the minimum it gives us the opportunity to operate over large ranges. Well, it's highly dependent on cyber, and you can talk about what we need are radios or whatever. That really does relate to what we do in the cyber domain.

For the Air Force, I think one reason why we have latched onto this with such fervor is we recognize that if we lose cyber and that control of cyber, then the operations that we do in air and space, we can't do. So it becomes very important to us.

The other point that you see there is really to talk about the same summary of what we talked about before. The last two bullets, it's a reality that what you're talking about in cyber is about global vigilance, reach, and power. It's a lot just like what we do typically with any of our air and space ops so it does come naturally for us.

As a matter of fact, if you take a look at what happened in the case of the control of the seas; you know, back in the 1800s, or maybe even earlier, one of the reasons that you started having a navy was that people started, these pirates would intercept the shipping and they expected the government to try to take some of this stuff under control. So when you do that, that kind of leads you to we need to have a navy. The reality is that 80 percent of our commerce these days is really being done over some form of cyber, whether it's the internet or it's over telephone lines or whatever else. So you have this potential in the cyber domain now to interrupt our ability to do commerce so this becomes very important to us and the reason why we have to think about how to defend it.

This guy here -- [Laughter] -- is our peer competitor. That is our peer competitor, because right now the cost of entry to basically do operations in cyberspace is relatively inexpensive; you need a broken pair of glasses and a laptop and you too can be a hacker and be a peer that's working in the cyber domain.

What the Air Force has made a decision to do is that we're going to do this like we do everything else in the Air Force. We're going to do this as a professional force, and we like to do things asymmetrically. You've heard before, in fact I remember General Jumper saying when we go into an air-to-air fight we're

not looking for it to be a fair fight. Well, we're not looking for this to be a fair fight either. So the way that we want to do this, we want a force that looks a lot more like this, like the Thunderbirds, and that's the kind of thing we're working towards -- a professional career force, weapon systems that are designed for us to dominate this domain and ensure that we can continue to warfight as an Air Force.

My clicker is not working here.

This was the task, and I got the letter that you see there, eight paragraphs, it talks about all the things. I really just wanted to pull the key points out of this. The first one I think it's important to look at this intent that the Chief and Secretary have which says that this is not just about setting up some new cylinder of excellence, if you will, some new stovepipe in cyber. It really is about extending our goal of reach and power into cyberspace, and it's about connecting these together and doing it so you can provide integrated global effects. In fact one of the paragraphs says that it's looking for 8<sup>th</sup> Air Force to serve as the Air Force's global effects integrator.

The third one is important because some people think that what we're going to do is we're going to sit back at some laptop somewhere and we're going to do cyber war. There is some of that that's going to go on. But the other part of what we're going to do, we are a force provider so we're looking to develop forces that can be sent forward to a theater to be integrated in a theater, to provide forces to deal with special operations, and in some cases to provide forces that can be integrated with non-military capabilities -- other government agencies -- to provide effects. I'm going to talk a little bit later about how we would do that.

The one that gets the most attention is this last one. We were asked to develop what was called an on-ramp for a major command that would basically do organize, train, and equip, advocate for cyber resources, and identify requirements in the cyber realm. We identified that on-ramp. That on-ramp has now become a provisional MAJCOM and I'll talk a little bit more about that in a minute.

A little bit about the cyberspace domain. It's not just the internet, and that definition that you see there that's at the bottom comes out of the National Military Strategy for Cyberspace Ops. I like to tell people that I use a triangle to describe it because most triangles I've ever seen have three sides, and there's three main parts to trying to do cyberspace to what's in there.

We're talking about the use of the electromagnetic spectrum and modulating that base within some way, shape, or form with

these electronic systems, but the reality is that there's an infrastructure that supports all this. For example, you have to have power for most of these systems to work, in fact all of them to work, and you also have to have cooling.

So when we take a look at cyberspace, one of the first things we have to do is we have to establish the domain, and so you see that there that one of the first things we have to do is establish the networks and that's really a part of what the cyberspace operation is all about. Then those operations in there do two other things. We either are going to exchange data, which is what we use the electromagnetic spectrum for, or we're going to store it or modify it, and that's what we use the electronic systems for. So it's a physical domain, but it doesn't exist naturally. So if you're now a cyber warrior, you can't go out and fight until you create your domain. So part of our job as a cyber command is to have the capacity to create this domain anywhere we want to warfight.

There's one other point I should make about the networks, by the way. The networks exist on several levels. There's a physical level, which is like what a LAN looks like, so it can be copper wires, or it could be fiber. There is what they call a logical piece, which is the routers and how things move, so that's a logical network. There's another element that is kind of the social networking piece that ties into this, because the ultimate purpose is you're trying to tie people together so that they can make decisions. So when we look at these networks, ultimately you're going to see us talking about what the role of cyber is in terms of doing influence operations, and it's because those networks exist on multiple levels that we care about that.

Here are some of the things that we're doing in cyber operations today. You may not recognize these as cyber, but if you have a radio controlled IED, if you can interdict the electromagnetic spectrum, jam it, or you can spoof it and keep it from going off, then you have done a cyber op. Conversely, if you're using that spectrum, and you're the bad guys, to cause these things to explode, then you're actually doing a cyber op as well that has a kinetic effect. And the obvious ones are there.

We run the networks for the Air Force, and we are worried about things like precision navigation and timing and the ability to spoof it and ensuring that our data, our networks, aren't tampered with because we have a lot of things that we're trying to do to prevent that. But all of these actually can be talked about as cyber ops that we're doing today. We're trying to move this quite a bit further on.

So what I would like to talk about is that people tend to think about cyber ops in one specific form or another and I want to just walk around this little set of circumstances.

When we talk about a cyberspace operation, the first one there you see is intel operations, and if you heard General Deptula a little while before, a huge amount of the intel operations we do are done through cyberspace. So whether you're doing signals intelligence or you're doing electro-optical intelligence from space, then you have to communicate it down, it requires cyber to do that.

Intelligence is not part of cyber, but it uses cyber to be able to actually effectively conduct that type of operation. Conversely, on the defensive side, we're very interested in the counter-intel piece, which is how we prevent an adversary from taking ours. And of course this idea of computer network exploitation, which is done by NSA, for example, is a big deal in terms of what we're able to do as a nation to understand what the possible threats exist to us by, say, a terrorist group.

The next one is information operations, and there's two parts to it there that you can look at. There's the way that they look at it from a joint perspective, which is the five on the right. Air Force, we look at it from the three on the left, which really look at the different domains that I have talked about with the networks.

The key point in this is that an information operation, it depends on the level, but if you think about this, we always worry about people stealing our data, but if someone could come in and tamper with our data, particularly decision-making data, that can be hugely important to us, certainly from a war-fighting standpoint.

Let me put it in a little different context. Suppose someone could go in and start tampering with your bank accounts; that would be a serious problem for you, particularly if people lost confidence in the information that was being stored that basically kept track of our financial networks and our banking. So information operations, both the defensive piece and the offensive piece is important.

I'll turn over to the business ops. Most people, when they think of cyberspace, that's what they think of is business operations. It's basically how we do all of our commerce. It's how we do our administration. Everybody in the Air Force, for sure, is involved with this thing because that's how we do our e-mail. You go to the website. These days, we now have a new verb, you can Google something and the thought that you wouldn't be do that, those operations are all done there.

We talk about those three factors that are important and that we're worried about; integrity of the data is not tampering with it, the availability of the data, that the network is up and

running; and then the last one, the privacy is that you don't want people to steal your identity basically, or pretend they're you when they're acting on the internet. The last one, though, one of the things that, so we do all those.

The thing that differentiates what we're doing in the Air Force compared to other agencies and even some other services is that we are now treating this as a warfighting domain, and we recognize that we are warfighting in this domain.

What I want to talk about now is what it means to fly and fight in cyberspace. We basically have organized it into three main areas. Believe it or not, it is a modification of a maritime model. So Julian Carbetz said that if you're going to do operations in the sea, the reason that you care about the sea is that you're doing something with it. So you have to use it, but before you can use it you have to control it. The difference with cyber is first, you have to establish it because, unlike the sea, it is not naturally there. So that's the basis of our model there.

So the first thing we're interested in, in terms of these operations that we do, is establishing the domain, which includes what we think of as network operations. The second part is how we control the domain, and there is a defensive and an offensive piece that I'll talk about. And then the last part is actually how you use it, so you can use it for force enhancement, which is how we help operations, in air and space or terrestrial for that matter, work better. We can use it for attack in and of itself, a counter cyber-type operation, and there is also support operations that we'll talk about.

So first of all, establish a domain; these are the kind of things that we do with this. It's fairly basic, but interestingly enough, when you think about something that happened with Katrina. I live at Barksdale now. When they lost all of their communications and everything, that was a big deal, and at the time the Air Force and a lot of other agencies were asked to bring in capabilities for first responders to be able to have a com capability. If you look at 9/11, one of the first things that the President was interested in doing was getting all the network up, the networks at Wall Street up so that Wall Street could open up on the Monday following 9/11.

So when we talk about this establishing the network, this idea of global expeditionary operations or cyber ops is that we want the capability to go anywhere in the world and have a robust network, and we're not just talking about a circuit. We're not just talking about a bounce up to a satellite that someone could interact with or jam, we want to have something that's robust, multiple satellites, air, terrestrial, all tied together so that

we can be sure that an adversary can't take away our ability to warfight by going after those com nodes.

There's a lot of stuff of here on the cyber defense piece of this thing. One of the points to make about this is that a huge part of our business is going to be defending the domain. I need to differentiate securing the domain, which we did in the other one. Secure is like putting up a fence around it and putting in an entry-control point, from defending the domain, which is more like what you think of in a warfighting operation; you have defense and depth.

I tell people that if you go to Barksdale Air Force base, for example, people, except for the security policemen, don't tend to walk around with M16s or revolvers. That's because it's considered a relatively safe place and you do the entry-control point and that's how you secure the base. But if you were in Balad, in Iraq, you've have defense in depth. You have people outside the wire that are out looking for adversaries before they would try to penetrate it, and then inside the wire itself you have people that are always wearing uniform, you've got your ID cards exposed to make it easy to figure out if someone has come into the area that you're trying to protect.

We're trying to do the same thing in the cyber domain, particularly with the Air Force parts of the cyber that we can control. If you look through that list there what you'll basically see is that we have to defend all elements of the cyber. You have to defend the electromagnetic spectrum first of all; you have to defend all of those electronic systems, which can be tampered with; and you have to control or protect the infrastructure, the power and the heating and cooling that allows it to operate; and you have to establish or protect the network itself. You have to protect those, both logical, the routers, and you have to protect the actual LANs themselves, so the fiber and the copper cable. If you put all that together, and you can see that it covers a lot of things, and you also notice there that we've got the social network protection piece of this thing, which is we have to defend against our social network being penetrated; that's where someone basically assumes your identity, for example, and there's ways that we can do that. That's what the CAT cards are doing for us now.

We also want to have an offensive capability against our adversaries. Basically, everything we are trying to defend ourselves with we want to do to the bad guys, so that's an easy way to look at it. But you can see the type of things we can do. We can go after the data itself. We can go after the operating code that makes those electronic systems work. We can use kinetic attacks against the infrastructure, so the power systems or the heating and cooling, and we can just use plain old jamming or spoofing. You can see any one of these things can have an

effect, or we can go into the routers and we can change the way the routers operate and we can, therefore, make a change in the virtual network. So there's a lot of ways that we can control our adversaries' domain. The best way, of course, is if you can do it and they don't know it. Usually if you drop a bomb on their power plants though, they have a pretty good idea of what happened.

We talk about using the domain. We talk about there's an OODA Loop -- Observe, Orient, Decide, Act -- that John Boyd came up with a few years back. What we're trying to show here is how important cyber is in terms of accomplishing this OODA Loop, and you can see that the first part of it is we use sensors to observe; we have systems that provide situational awareness where we integrate that data together, we then make decisions on that, which is where we do this operational integration; finally, you bring the actions together to create effects.

Now what happens, that cyber is what allows us to operate over these large distances and to be able to, for example, send a B-2 out 40 hours before it's going to hit a target and make a target change before it gets there. But if your cyber is restricted and you don't have the bandwidth to do that, then that's going to limit just how much flexibility that you have and it's going to have a detrimental effect on your ability to operate. The same thing is true of our adversaries. Oh, by the way, each of those different pieces, you can go after that. So you can take the cyber out completely. You can go after the sensors, you can go after those fusion systems, and you can do things to affect how they integrate their data or actually even how the weapons systems operate to create an effect using the cyber domain.

The other part of using the domain, though, is first this kind of this force enhancement. This is talking about how we can take that data that we just talked about, and if we have a way to bring the data together in a way that we can make adjustments quickly, that's going to help us obviously. We're trying to link our AOCs together, so that theater, special operations forces, they're interconnected and we have a global picture that then can be integrated in any AOC.

Then the last one is that we don't want this to be a stovepipe, so when we have a, for example, General North is doing an operation in CENTAF in Iraq, and there is a global cyber capability that's available. We want that integrated in the theater.

Then the last part talks about the cyber ops. I can let you read that, but you see we do have to support these things and these aren't specifically cyber operations but they are things that we can support through cyber, and a couple of them I'm going

to hit just a little bit more if I can get the slide to advance here.

We always talk about what's the thing about sensor and data integration. What we're trying to do is use a thing called service-oriented architectures, and the idea is that we want to be able to get to authoritative data; we can protect it better that way. So when you hear this discussion of moving from web-enabled, which you see on the left side, to service-oriented architecture, where we're actually able to integrate data rather than just put a number of displays on one display or one LCD or whatever, the big advantage of this thing, though, it it's very orderly.

So when we're trying to do protection of this environment we can see all the data movement, so it allows us to protect it better. It's hard to move to this. It's all about doing data sharing, and the big challenge we have is we're trying to push to share more data but the more you share it, theoretically you expose it to vulnerabilities, and the service-oriented architecture is the way that we can get around that and protect it better.

When we talk about operational integration, when we talk about bringing these AOCs together, the chart is complicated. The part I want to highlight here is that when we have a cyber effect, even if it's a global cyber effect, or a global cyber capability I should say, we're looking for a theater effect. We're looking for the theater AOC to integrate that, so the Theater Commander of Air Force Forces is going to do that integration, and so you see all those different capabilities that are there that can be brought to bear. Right now, we tend to bring these in as, we call them stovepipes, and the theater COMAFFOR doesn't have a chance to integrate it. What we're trying to do is establish with these linked AOCs the ability for those global capabilities to be integrated in theaters.

And we're doing this defense industry support. You may have read some of this. We have done some pretty good work in the Department of Defense in terms of protecting our sensitive but unclassified information, and we have gotten so good at it, in fact, that the bad guys have figured that it's easier to go after our defense contractors instead. The reason is that we have access to a lot of information that we get through the intelligence community that the defense industry doesn't have, and yet they have a lot of the same information that is of interest to our adversaries. So we're working, and this is not just, it started out as an Air Force program which has now expanded. It's a Department of Defense program which we're playing a very active role in to help our defense partners protect our data as well as theirs with greater knowledge of what

the threats and vulnerabilities are and also what kinds of capabilities can be brought to bear.

The key point of this thing is that we are able to bring in the intelligence community, law enforcement, and our sister services and now share things that before weren't being shared, and that's really where the biggest benefit is coming from.

Now we want to talk about warfighting. This is a cyber terrain map. So if this were, you know this isn't a map of Iraq, but if you're trying to look at the cyber terrain, this is kind of what it looks like. Basically, we're the blue, we're the good guys, and the bad guys are in red. Part of the complication as you go through this thing is you see the network that we're actually responsible for are these DoD networks. As you get further away and it's not government, what we're able to do with these networks shifts, to where you have kind of a neutral zone, almost like hockey, and then you have your adversaries' cyber, and if it's clearly an adversary cyber there's a lot of things you can do, but then you've got these zones where you have to worry about the fact that it's commercial-type cyberspace. All these are things that we're working on.

It's no different than rules of engagement that you would need for any other type of operation that you would do for warfighting. The first thing is to understand kind of what the terrain looks like. So when we talk about the cyber terrain, this is the kind of thing that we're looking at.

So now, when we want to talk about how you would actually pull these things together for some type of war planning, for example, and we're worried about offense and defense so this is a little different triangle than the one that I showed before. You see we have the electromagnetic spectrum; we have the infrastructure. In this case, though, we've got the infrastructure being both the electronic systems and that basic infrastructure. Then we're talking about the data.

The reason we're doing this, this talks about the different types of attack that we can use and also the different types of defense that we need to have. And you see there's your three different, or four different types of networks. You've got your wireless networks; you've got digital networks, which are the logical nets; your physical networks; and then you see inside the triangle, that's that social network that we're concerned about. So if someone's going to attack either us, or we're going to attack them, these are the types of attacks. You go after those four different types of networks.

Conversely, if you're going to protect yourself or defend yourself, you have to come up with defenses against each of those types of attack. So you see, you can have kinetic attacks, you

can have electronic spectrum attacks, and you can have what is traditionally thought of as a network attack.

A key point of all this is that how you do all this, this refers back to that terrain map. It depends really who the actor is, who is it that's attacking you depends on how you can defend against it and the type of adversary you're going after. Whether it's in peacetime or it's actually a war situation, is going to have an effect. Is it self defense or is it offense? And then, finally, what are the specific rules of engagement? These are all the kinds of issues that we're working with, largely in conjunction with STRATCOM and with the Joint Staff and OSD for that matter.

This talks about, I love this chart because it's got a lot of, this is how 8<sup>th</sup> Air Force integrates into STRATCOM. What you see there, 8<sup>th</sup> Air Force, is also the component to STRATCOM for global strike and integration. We're the component for network warfare, and we're the component for Global Network Ops. But then we also, because of the cyber influences in terms of global command and control for the integrated missile defense or for ISR and for the information ops that the JIOWC with the Joint Information Operations Warfare Center, we have relationships with all of those to help ensure that we can provide a good Air Force component for those joint operations.

What you see there again is that we provide direct support for a theater-functional commander of Air Force forces for the types of operations they do. We look for the operations to be integrated in that other AOC if it's not a global operation.

So now, the provisional MAJCOM. Everybody's excited about provisional MAJCOM, including me. What you see on the right-hand side, where you see that AFSTRATC, that's AFSTRAT Cyber-Strike; that is the name of the Air Force component to STRATCOM for doing cyber and global strikes. So all those things I showed you on the spider chart all captured in that one box.

We have an Air Operations Center that operates 24/7, that supports the operations. And we have an 8<sup>th</sup> Expeditionary Task Force which was set up because a lot of the forces are in other MAJCOMs. In fact, they're all in other MAJCOMs, so they're either in ACC, or some are in USAFE, some are in PACAF, and what we have to do is we have to have a way when they are doing operations in support of STRATCOM, we have to have a way to realign. And so the 8<sup>th</sup> ETF allows us to do that.

Then, administratively, you see there are these wings assigned to 8<sup>th</sup> Air Force, and so 8<sup>th</sup> Air Force reports up through Air Combat Command for the administrative control of those wings and provides what they call administrative control of the forces assigned to do operations in support of STRATCOM.

What you see on the left side now, highlighted with the yellow, is we took the on-ramp that you see there and that now became the AF cyber provisional, and the capabilities that are being used to do that are coming from the Air Force Communications Agency, the Global Cyber Integration Command, and ACC, as well, is providing capabilities out of their A3I shop, which is information ops and then 8<sup>th</sup> Air Force. So that was the on-ramp to the MAJCOM, and now Major General Bill Lord is going come in to be that provisional MAJCOM commander.

What you see there is all the operations part; that's what you see on the right side, because there is no change there. What's different is that on the left side, for purposes of developing programs and for trying to advocate for requirements or identify for requirements, that's going to be done through this provisional command straight up to the Secretary of the Air Force through the Chief of Staff. And the point of this is, to give cyber, you remember the Secretary said he wants cyber to have an equal place for advocacy along with air and space, and that's how we're doing it in the midterm, is to use this relationship.

And the one other job they're going to do, by the way, is forced development action, which is that cyber career force we were talking about and working to actually develop the program action directive that will lead to the permanent MAJCOM. It will be busy.

It's interesting, you know there's a lot of talk about so where's the cyber command going to go. Well right now it's in a lot of places anyway. So there's a C2 headquarters that's at Barksdale, but the reason we've been able to do a lot of things already is because the Air Force had a lot of capability in the cyber realm already, and if you take a look around here, and there's actually others that could be listed, these are all of our, we call this our cyber enterprise; these are all people who are doing things that are cyber related that we now basically have pulled all these things together and are able to, particularly when you're talking about research, you're talking about Electronic Systems Command, which I don't even have specifically listed up there, that does our acquisition for us, as an example. The work we do with Space Command in terms of integrating the space ops. The work we're doing with Langley in terms of doing theater ops.

So it's a big enterprise already, and what we're trying to do is grow this thing, particularly with the Guard and Reserve, because it's a perfect Guard and Reserve mission. So we anticipate quite a growth in some of the Guard capabilities that we are going to try to add to this overall enterprise with

individual Guard units focused on specific capabilities that would help the Air Force fly and fight in cyberspace.

These are some of the initiatives that we've been doing. We've talked about what we've done already. There is one that I think is worth highlighting, which is that we have tried to approach this thing just like we would a flying operation. And so we said, you know we can do safety programs, we can do StandEval programs, we can do operational risk management, and we even have a program, we call it the Cyber Sidearm Program, which should be unveiled here, we were shooting to have it out before the convention so we could show it to people. It took us a little longer.

What this is all about is just like I told you that if you're at Balad, people carry M16s or they carry a sidearm to help defend the base if it's attacked. Well, we're being attacked in the cyber domain all the time. So we want every airman to have the capability to help defend the domain, and the way we're going to do that is with a program we call Cyber Sidearm. And all these other things really show you just how busy we've been in terms of integration with the Air Warfare Center, for example, or work directly with OSD and the intel community on this President's Cyberspace Defense Initiative, which we have been invited to participate with.

The foundation for the future. That's our requirements, that's what we've said we're looking at, and General Bill Lord is going to be working to refine those and put those requirements to some great specificity. In the '09 amended POM, our focus was on increasing the survivability of our networks, and we were able to move quite a bit of money to really focus on doing that.

If you look at what we're currently doing at 8<sup>th</sup> Air Force right now, you see that, in terms of our focus areas, that's where we're currently focusing our attention so it's kind of a way actually to see kind of some of the differentiation in terms of where we're going to focus attention. So General Bill Lord is going to be focusing on those requirements and getting those into programs, and our current focus areas are to make all this happen with the capabilities that we have already.

So this is kind of an attempt to sum all this up very quickly. It's not just about doing cyber ops; it's about integrated air space and cyber ops. And we're doing it today.

We have a 24/7 AOC that's operating at Barkdsale and working in conjunction with the Ops Center that's at STRATCOM. It's all about providing freedom of action, because the Air Force absolutely must have freedom of action in cyberspace to do its job.

We are working to link all AOCs, not just the theatre, but the Special Operations and the global and functional AOCs as well. Part of this is to be able to leverage all instruments of national power, not just military. So we want to be able to work with the diplomatic and informational and economic instruments. And we're having pretty good success that way.

And then, finally, we know that if you're really going to be serious about this, it's going to require new competencies and we are working right now to develop new career fields. These will be new AFSCs that we hope to roll out this fall actually with cyber operators that are basically married up to some cyber weapons systems that we're trying to formalize.

The other thing we're doing as we look to the future is we've got some great partnerships that we're working with, with industry and with academia as well. And a combination of all this, what's really interesting about this is that a lot of people have been doing work in this area. I think one reason that they've been attracted to us is that we're willing as an Air Force, from the Chief and the Secretary on down, we're willing to raise up our hand and say we are willing to put the resources that are required, the commitment to pull all this together. A lot of people who have been interested have basically formed up on us and, as a result, I think we've got a pretty good program in place now and I think as you look in the next few years, you're going to see this grow substantially.

So I did this quick, a quick run-through, trying to tell you all about the different things we're doing, but I'm happy to take questions and talk to you in a little bit more detail because we are flying and fighting in cyberspace today. So thanks.

**Question:** How long do you think it will be until you have [inaudible] capabilities in tactical aircraft that might be able to take advantage of their stealth [inaudible] to get close to [inaudible] and be able to --

**LtGen Elder:** We actually, we practice those. I told you about the stuff that we do at the Warfare Center, so we do those types of things right now in the mission employment phase; for example, coming out of the weapons school, and we're in the process now of starting to bring it into the different flags; Red Flag, Green Flag, and a new one we're looking at called Black Flag exercise. So we are actually starting to practice those capabilities with an intent that we'll get enough confidence that we'd be willing to offer that up to a COMAFFOR in the future.

**Question:** Do you have any sense of what tactical units might need [inaudible]?

**LtGen Elder:** Not specifically, but basically your stealth platforms, as you pointed out, are going to be one of the keys, but that's not the only way that we can do this. Remember, this is about integration of space as well so we're working with UAVs, we're working with space, and we're working with the fighter and bomber aircraft. We've got the big ISR platforms, like the Rivet Joint get involved. Actually, one of the platforms that has been doing a lot of great work for us in this has been the JSTARS, so it's not restricted to any one platform.

The best thing to do is you put these capabilities together, you've got these guys that have been sitting at weapons school going through all this training, and they are really geared up to be able to do smart things. It's amazing. It's unfortunate that we can't talk about some of the things they've done in this environment, but these weapons school graduates in their mission employment phase, the graduation exercises, we'll have been able to put some great capabilities together today. And now what we're trying to do is institutionalize them. That's not really my job. That's actually Mike Warden's job.

**Question:** So is Black Flag going to be primarily cyber?

**LtGen Elder:** No, no. Black Flag is a capability that the Warfare Center is working to develop, where, because of all the things that you set up for that ME phase, the Mission Employment phase, what they actually want to do now is take some of their highly qualified instructors and some of the test capabilities that we have, because the things that are still in development, you don't let the ME phase guys use those because it's still in test. So on the Black Flag, you'd now put your very best instructors at the weapons school and some of our test outfits together to try out some of the capabilities that we have to get a good idea about where we should be putting our resources and to get some experience with it. Actually, the right guy to ask about that is Mike Warden, Wardog, so he's, that's his program.

**Question:** General Elder, this was informative. I'm trying to look ahead to the day when it's no longer Provisional Command and it's a true MAJCOM. Currently, you now have 8<sup>th</sup> Air Force, you have a cyber wing with forces that you've chopped to STRATCOM. When this cyber command is fully operational, will it have forces [inaudible] or are they going to stay within the 8<sup>th</sup> Air Force?

**LtGen Elder:** A little of both. With a permanent MAJCOM, and that's one of the things actually that the provisional MAJCOM is supposed to sort out, but the idea is to have what they call a MAJCOM component similar to USAFE, to EUCOM, or PACAF to PACOM. Well, this would be a command that would be aligned specifically with STRATCOM. It won't be the only one because you're still

going to have AF SPACE, but it will be aligned to bring these cyber capabilities day to day, so network-type operations is an example, information operations, the things that are being done on a routine basis day to day by STRATCOM, they are now already aligned. You still have to have what they call an execution order to do all that, but we still will have this capability to pick up forces and deploy them where need be, and we also will have capability to deploy in place, similar to what we do at Nellis right now with flying the Predator, so even though they're at Nellis, you know when they're actually flying the Predators they're working for CENTAF there in the AOR, so it's going to be kind of a mix of both.

Then the other part that we're doing is, and what we anticipate is that a lot of these capabilities may actually be cyber capabilities that ride on some other platform. For example, you might have a transponder that's riding on a tanker, for example, that allows you to have an airborne network. We're not responsible for the tanker itself, we'd just be responsible for this transponder that's on it.

It's interesting, by the way, that the FAA is way ahead on this. They're looking at a capability right now that they think will improve their communications, allow them to put airplanes closer together for intercontinental air traffic by mandating a new transponder that will set up an IP network across the ocean just by going from airplane to airplane, and every airplane will have perfect knowledge of where the other airplane is. So instead of having to keep these large distances between the airplanes that we do now to make sure that they don't hit each other, you'll have a network that automatically does it, and it will be no different almost than what we're doing, see and avoid.

So the capabilities that you have once set this thing up will be pretty significant, but once again we're trying to integrate it with air and space, and just because it's on a satellite or it's on an airplane it doesn't mean we have to own the airplane or the satellite; we just need to make sure that we have a capability to establish that network.

**Question:** Certainly this is a necessary activity, and it's been recognized by many of the services before the Naval Security Activity's implemented things like this with active groups and started developing personnel resources, and they expanded that into the Fleet Information Warfare Center and so this is something that is necessary. But I just sat in to a briefing on recapitalization and the cost of that; the budget cuts that are impacting the space assets that are trying to get up on station.

How does this work into the balance of the financial resources available? To do this, we've go operationally responsive space as well getting money added into that.

So how do you balance all this out, and where is that money going to come from? What's going to lose to do this?

**LtGen Elder:** We hope nothing loses. [Laughter]. Interestingly enough, I can almost turn this around. Part of the reason that you need to take this approach and part of the reason you're looking for this kind of advocacy is as you are looking at how you do things in either air specifically or particularly I'd say the CAF, the MAP, space, it turns out that there is one thing that they all have in common. They are all using this cyber domain. There are some areas where we have a lot of redundancy, and we have other areas that have these huge shortfalls. So part of this MAJCOM's job, by the way, we haven't focused on that too much; that's really what the MAJCOM gets to focus on, which is really how do we make sure that we have this cyber capability?

A good example, when you talk about the operation responsive space, we need that very badly by the way, but when the Chinese launched the ASAT, everybody said well this is an indication we need operation responsive space. I said no, we needed operation responsive space before they ever launched the satellite. What this tells me is we need airborne networks, because if you want to deter a Chinese ASAT launch, and they're able to go against information services, what they're really doing, that ASAT launch, although it went against the satellite, was really a counter-cyber attack, because what it was showing you was that I could take away your ability for information.

But if I want to deter that attack, one good way to do it is to deny them the benefit of the attack. So if they take out the satellite, I can provide the same or very closely the same capability with an airborne platform or a mixture of an air and terrestrial network, and they take that out then you're going to say you've made really mad but you haven't taken away my cyber capability.

So when we look at those kinds of things, that's what we're looking at as we're saying can we provide some of these capabilities in a way that won't break the bank, quite frankly, and oh by the way, as it turns out some of the ways that you actually increase your protection reduce cost. It seems counter-intuitive, but a lot of the things we do right now, like for example, every base has its own set of servers. They exchange servers for e-mail and web services and everything else. One of the ways that we've significantly reduced the tax on our public web services is that we've centralized all that now, and we don't expose our actual web servers to the public, so we actually go through a commercial firm that puts all of our public web services all over the world, and if you attack what looks like our website, you're really not attacking our website, you're attacking a replicate of it, and if you take it out, it's not big

deal. They just take that one down, and then there's another 1,100-some left.

So a lot of what we're doing is really not about adding cost but realizing that each of these different major commands, each base, let me give you another example. Right now we have 132 gateways to the internet that we operate, and each of those gateways has to have people that manage it. We're reducing that to 10, and when you reduce it to 10 that significantly reduces the manpower that you take that are controlling those gateways, and we've learned a lot from commercial practices. A typical, our Network Operations Center right now takes about 300 people to operate one of those. Commercially, they're able to do that same mission with about 30 because they put some things in with automation and standardization.

So a lot of what we're looking at, we're actually doing it to increase the effectiveness, but we have this nice condition where as we increase the effectiveness it's actually going to reduce the cost. I can go on with a couple of other examples, but the bottom line is we don't see this as something that's going to specifically keep us from doing other things. It's actually going to potentially enable us to do things and make some money available.

**Question:** Thank you for these [inaudible]. [Inaudible] potential [inaudible], how will you address this and how are you going to cope with the fact that some of your allies will be ready; some others will not? Thank you for your answer.

**LtGen Elder:** It's the same problem that we have kinetically, as you know. So, I mean one of the issues we had in Iraqi Freedom was that a lot of the capabilities that we had, we had to be careful how we used it to make sure that the allies that we were working with, we didn't disable their abilities. The way we did it in those cases, we did it with processes or procedures that would, for deconfliction.

One of the biggest problems that we have right now, as you know, is multilevel security and the ability for us to share information across different countries. Technically, we have solutions to allow us to do this; we just haven't figured out the policy that pulls all this together. It is a huge challenge, and there's a lot of people looking at it. It really is a good question. When we actually start working with our allies, which is one reason why every chance I get we're trying to bring some of our allies to work with us, because the more we work together and we force the problems, then that gives us a chance to try to find ways to fix it.

But you're right, particularly when we go outside of a U.S.-only network and even when we go outside of a U.S.-only military

network, I mean we actually have this problem when we got not just outside the U.S., but if we go from a dot-mil, which is our military network, to a dot-gov, we have issues there, configurations and everything else. So it's something that has to be worked, but I envision that the way that we do this is going to be no different than the way that we prepare for any type of coalition operation, which is we look at what the capabilities are and then we're going to have to actually design a system, you know, the equivalent of airspace control and those types of things, just as we would have for fighting AirOps, we'll do the exact same thing for cyber.

**Question:** Sir, unlike kinetic wars, what kind of metrics will you use to tell you're winning the cyber wars?

**LtGen Elder:** Well, there are some that are more obvious than others. We're actually trying to develop capabilities now; we already track how many probes we get, how many we catch, those types of things. We're trying to put systems in place right now.

This what's called a Combat Information Transport System Block 30, nice easy name, acronym CITS Block 30, easier to say. As we go into the spirals down the road we're going to start setting up these clusters. I told you we were going to move away from all the bases having their own systems, for example, and we'll have clusters of networks where we can actually compare.

So, if you think about if you're flying an F-16 and you have a problem with one of your flight computers, the way you know that there's a problem is that one of the other two flight computers say I've got two that say the same and the third one is different, and that would be an indication that that thing was attacked. So one of the ways that we're trying to do this is trying to build in these redundancies. We talk about taking an approach that moves from information assurance to mission assurance, and we're not only interested in what's being stolen in terms of data but how we protect it.

So a lot of this has to do really with the systems that we're putting in place, both for redundancy and for resiliency, we're going to be able to track more information. But in terms of if you're in some type of a conflict, if you want to go to the high level, if we're still able to do our AirOps and our JDAMS are dropping on the right place, and we're able to complete an effects chain of find, fix, track, target, engage, chain, as long as we're doing that, that's a pretty good idea that we're successful. If our adversary can't, then we've been successful from an offensive standpoint, but at that lower level, as we develop these systems that we're able to monitor much more carefully and we have comparisons, it won't be against a baseline but against each other, I think we're going to get a much better

idea of how well we're doing in terms of protecting and operating the network.

**Moderator:** Sir, thank you. It's obvious we could go on for hours, and we appreciate all the information you've shared with us. The Air Force Association would like to present this book to you in response. It centers on the memorial but also the history of the Air Force. Thank you so very much.

**LtGen Elder:** Thanks for having me out here. [Applause]. Thanks to all of you for coming.

# # # #