

TRANSCRIPT

## Defense Writers Group

A Project of the Center for Media & Security  
New York and Washington, D.C.

---

Lieutenant General Robert J. Elder, Jr., USAF  
Commander, Eighth Air Force  
June 13, 2007

THIS IS A RUSH TRANSCRIPT AND MAY CONTAIN ERRORS. USERS ARE ADVISED TO CONSULT THEIR OWN TAPES OR NOTES OF THE SESSION IF ABSOLUTE VERIFICATION OF WORDING IS NEEDED.

Q: Welcome to Lt. Gen. Robert J. Elder Jr., and he's commander of 8th Air Force, but (proof that no good guy goes unpunished) he is also "joint functional component commander for global strike and integration, US Strategic Command." Anybody that wants that on paper, I've got it here. (Laughter.) So welcome, first time in.

A: Thank you, it's great to be here.

Q: OK, take some time here and bring us up to date on what's happening in cyberspace.

A: I'll tell you it's a, I think this is an exciting time for the Air Force--we have a mission statement that said that we're going to stand up (inaudible) mission area of cyberspace and really make it an integral part of our mission statement. It was back in December 2005, so this has been in the works for a while. I think a lot of people wondered, including me, because at that time I was in a different place. The mission statement said we were going to fly and fight in airspace and cyberspace and little did I know that I was going to be the one who was leading the fly, fight in cyberspace piece, but that was the recognition really (inaudible) Chief and the Secretary that cyber is so integral to what we do in the Air Force that we're already heavily involved in it but we really needed to organize as a service to fully exploit that, that capability. So, that was the beginnings, and then last November is when I got what people refer to as a go-do letter which said here are the things that we want you to do in terms of standing up this command. And the (inaudible) pieces, a lot of people focused on the standup of a global effects majcom, which we are working on, but sort of my primary task was warfighting, and that's really

what this is all about. It's about a recognition that everything that we do in the military actually, and you can extend that more broadly but it involves cyber operations and that we in the Air Force needed to fully integrate that into what we do with air and space.

So while on the one hand we started, we said we're going to formally stand this thing up the reality is that within really a few weeks the task (inaudible) and I will tell you today a little bit about some of the things we've been doing. So the first focus was on a warfighting headquarters, if you understand we're establishing these component headquarters and this one's really focused on 8th Air Force and we still have our strike mission, but for now integrating this very closely with what we do with cyber, and we're working to integrate that with space as well. So all of that's in progress--(inaudible) program action directive was signed sometime back for all the component headquarters, and our organizational change request is in place and it should be signed sometime this summer and we will formally stand up this component headquarters to support STRATCOM and provide not only strike but the cyber capabilities to STRATCOM, but also we'll provide the same capabilities through the theater commanders, so my counterparts throughout the theater, the force providers.

And what's interesting is while the formal organization isn't there, we're starting to do this already. So the organization piece is coming together from a training standpoint; what we've recognized is that if you're really going to take this on, and look at everything else we've done in the Air Force, (inaudible), and in our early days of space there's a lot of research that went on and we tinkered with it and actually in some ways it's what we've done in cyber but we're looking to set up a professional cadre of cyber operators, and this would be enlisted and officer, and the idea is that we want to bring people into the Air Force from the beginning knowing that they're going to be a cyber operator and they will have a complete career path in the Air Force doing cyber.

Hopefully, 25 years from now if you're still up here doing these breakfasts and you're going to talk to the cyberspace czar, he will come into, he or she I should say, I don't think it'd be a robot (laughter), but he or she will commit to the Air Force (inaudible) and likely will have done this for the entire period of time, so we're working in the Air Education Training Command. One thing we're very proud of in the Air Force is our education training programs, so we expect that to truly take hold here very soon, and then there's a part about educating every airman to be fully aware; part of what we do with cyber just as we do with air and space.

And the other piece is just as we do with everything else we're trying to look at this for a weapon system approach, so if you've heard me speak in other places where I've talked to industry, I start talking about how we're trying to move away from these ad hoc different approaches that (inaudible) to a professional approach where we have standard systems that are working to do these types of operations and all this is in motion and as

we are doing cyber ops today and all of these different parts are in place, one thing that the Secretary at one point noticed was that he went around the Air Force, he calculated roughly that there were about 40 thousand people that were involved, this is officer, civilian, and enlisted that were involved in cyber ops at one point or another but they were scattered everywhere and part of his effort was we really need to appoint some kind of a cadre really get the (inaudible) synergy on this. A lot of this is really about shuffling to maximize the effects and again my task if you look at it is to provide this capability to STRATCOM, to the theater COMACCs, (inaudible) provide for interdependent joint ops and to move from the idea that what we do with cyber or comm. or anything else is just to be an (inaudible) function we used to actually make this part of how we warfight. Our adversaries are doing it, and we want to take advantage of the might and the intellect of our nation just to get ahead of them. That's kind of where we are.

Q: OK, so when is the command going to stand up?

A: I expect that the warfighting commands, my three-star commands, should be in place sometime this summer. It's a matter now of, as I said, the organizational change request is going through the system, and remember, this is part of a larger program action directive which was taking all of our, for a period of time we called them warfighter headquarters, but the operational headquarters, standing those up, and in Air Combat Command we expect those all to come sometime this summer.

Q: But I'm talking about the new major command--

A: Oh, major command. That time, I'd say, my direction was to work the on-ramp for majcom and my piece of this is in place now, so for me, the on-ramp was forced to be able to be involved in the resource drills. So for example, getting ready for the '08 budget in terms of execution, money, and to actually be able to influence the '09 amended POM. And so my job with this on-ramp was to make sure that we could add the (inaudible) cyber resources, and that was actually one of the early things that we did, so that part of my tasking in terms of putting I guess the formal piece in place so that when the Secretary and the Chief decide that the timing is was right and they know what all the political things or anything else involved that they're working will be ready, and so we have people that we've brought into 8th Air Force already, and actually (inaudible) more this summer is they're really there to support these on-ramp activities, not just a matter of when the time is right.

Q: So this summer, if all the pieces would be in place, whenever somebody wants to turn a key, it could be then, it could be in the fall?

A: Well, in terms of actually standing it up, it depends on exactly--part of the issue is

they're still trying to determine exactly what this global effects majcom what is going to be part of this, but in terms of having the capability to do typical majcom activities, which is advocating the resources required in the program, we should have that all in place at the end of summer or fall. So then it's a matter--but I tell you, it's taken us a year to this component, the operational component, it's a taken year to do that so it's one of these things they don't happen over night, so once they decide that we're going to do it there's going to be some period of time to staff it all and all the things that have to happen with OSD and the Congress--it'll all take time, but we'll be ready.

Q: General would you describe what cyber warfighting effects you want to accomplish and give us a sense of where the United States stands in terms of capability vis a vie potential adversaries or anybody else. Where are we (inaudible) and how much money are you spending?

A: Well, I tell you that I don't precisely know exactly how much money that we are spending right now. If you go across the Air Force budget, in effect, you go across the Department of Defense budget, look at all the things that really are cyber-related it's a lot of money. It'd be hard to pull all this together but--when I tell you when we look at cyber warfighting (inaudible) to explain to someone what we think is involved with that, because it's actually pretty big enterprise effects, when we can talk about it I tell people, some people will look at cyberspace if you come out of an intel background and you say, well, cyber, that's what NSA does, for example, because they go out and they do computer networking (inaudible) is part of their collection mission and that would be true; that's one piece of it.

If you talk to the, historically you thought of cyberspace with the information operations kind of a framework which is really how the Air Force has been approaching it in the past, and in this case you say, well, this is really about just computer network attack, and by computer network attack we say we're going to go in and do traditional information operations functions like military deception or cy-ops, those types of things, and that element is still there, but there's no recognition that what we do in the Air Force is we use cyber, we always have to enable the way that we warfight and now we say it's not just a matter of enabling it actually is part of the warfight.

In fact, we really follow the DOD definition for cyberspace, which is pretty broad. It says that it is a domain that's characterized by the use of electronics and the electromagnetic spectrum. That's when it goes on to claim it is to create, store, and exchange data over network systems and its associated infrastructure. We put all that together so that's cyberspace--in fact, someone said well, basically you're taking over the whole Air Force, but that's not the plan (Laughter.) it's not mine, I think it might be somebody else's. But the point is that it's fairly broad. For us, though, what we kind of recognize is that the Air Force has been doing interdependent joint ops for really a long time, since our

beginning, and what is always enabled us to have it is we now recognize in today's definition cyber. So we are big proponents of centralized or decentralized execution, you've heard that before. And we look at that in terms of giving us the speed and flexibility, agility, over large ranges, it's all because of that cyberspace, so if we have an adversary that can go in and could take away our domination of cyberspace then what they would, for the Air Force it means taking away speed, range, and flexibility that we provide to the joint force commander.

And what you lose with that is not only freedom of action in the cyber domain, you lose freedom of action in every domain, so when you look at this thing, the primary focus of this right upfront is to make absolutely certain that we can control the domain just like we want to control air, we want to control space. We have to control the cyber domain and we're not going to do this alone. Everybody's got to be a part in this, but we have a critical role to play because for our own use we absolutely have to have domain control. If we can't communicate with the aircraft, if we can't communicate with spacecraft, we can't do our mission. Some other services, other agencies you can pass notes or you can walk over and drive a car, we can't do that.

So it's very important we have that, so when we talk about, what we're trying to do when we say in the warfighting context, it's a little different than other people looking at it in terms of just trying to protect your business system and say which for us is a big piece of what we're doing as well, and that kind of falls into what we typically call our network operations piece, but that's important. We're really worried about how do we control this domain so we can continue to operate as an Air Force and provide to the joint force commander these effects that they've always had basically, since the Korean War, since anyone on the ground's been attacked by an aircraft.

Q: (Inaudible.)

A: Well, here's some specifics that you can think about. When you look at those areas there; where people tend to want comparisons in the area of this information ops, you might take a look at some of our potential adversaries. We have peer competitors right now in terms of dealing with computer network attacks through computer network exploitation--and I believe that we're going to be able to ratchet up our capability to where we put the intellect and the technological might of the nation to do (inaudible) moving us away from the equivalent of everyone else which is the backdoor garage mechanic type approach to this thing. We're going to go way ahead, but then look at these other areas that we're talking about, and we are way ahead in terms of--there's no other nation on earth that can go through any part of the world--we always think about our expeditionary capability in terms of what we can do, in terms of moving people and equipment any place in the world. You have to realize we can go to any part of the world and we can start doing operations immediately because we can stand up the

communications, the command and control systems, situation awareness systems, that we need to be able to do that.

That wasn't the case back in the 1990s, if you think about it, we rarely moved people and equipment over for Desert Shield/Desert Storm. A real hold-up in terms of getting that thing moving was getting all the command and control structures into place. Nowadays, we can go anywhere in the world and back in the time it takes for a spacecraft moving overhead or for an aircraft to fly there, we're prepared to do operations. The connectivity that we have is unmatched, and so when we think about using cyber for warfighting purposes, that's what we're talking about is this ability to have this the Air Force (inaudible) global vigilance with the situational awareness all over the world, the ability to move forces and gain even greater situational awareness, to command and control these forces, and then integrate with these capabilities.

When you recognize that this is an integral part of what we're talking about with cyber and then to be able to do interdependent joint operations, which means that, even though we've traveled some incredible distance, we can deal with a coalition member on the ground. We can deal with SOF forces. We can deal with other agencies. And we can do it on the fly. So part of what we're doing, we recognize we have this tremendous capability and when we talk about defending, when we talk about cyber defense, we're not just talking about trying to fit some kind of better virus protection on a computer, we're talking about protecting this ability to do these interdependent joint operations, and so when you say, how much money's going into that, I mean, a huge part of the Air Force budget really goes into this, and there's a recognition that we've been doing this for a long time, and that No. 1, it gives us an asymmetric advantage--if you're an adversary and you recognize that the United States has a asymmetric advantage in this area, your adversary's going to try to take it away. So our job is to make sure that you defend it. So a lot of attention on being able to preserve these capabilities we have and in fact even advancing those capabilities further.

Q: What type of technical background are you looking for for the airmen you plan on bringing into the cyber career paths and what kind of training?(Inaudible.)

A: If we have a whole tiger team that's working--it's actually being led by the Air Force Institute of Technology (inaudible) and some people that are very good at doing this, and just as we have a span of different specialties, if you will, that support air and support our space operations there's going to be a range of specialties that support what we do in the cyber realm, so there's going to be some variation. If you take a look at what we're looking in terms of bringing in officers or civilians, I'd say, from an education standpoint, we're going to be looking for people that have these technical-type backgrounds, whether it's the computer science or electrical engineering or some of the hot ones, we're looking for people who have been educated in the use of computers,

networks, and also (inaudible) electrical engineers.

If you look at the training piece, we're working with the Air Education Training Command right now and one of the things we recognize for those of us, say, my age actually, and below the age of maybe 25, used to doing these things--my daughter can be doing a conversation with me and all of a sudden she'll show off to me and my cell phone will buzz--she just sent me an SMS while she's talking to me without looking at it; I can't do it when I'm looking at it (Laughter.) you know, I don't know about you. So what we recognize is that our young people in the United States have a great talent in this already and some have more than others, so what we're talking with Air Education Training Command now is that people that come through our basic military training. This is being done already because of other career (inaudible)--they'll start looking for who has these kinds of aptitudes and actually look for people who have a natural capability to do this and then try to funnel them into areas that take advantage of it.

But we also recognize that for this really to work it's going to take some significant training and so that we'll take these people, put them into formal training courses and they're still trying to define that, and it's interesting, they've looked at a range of different programs, this is Air Education Training Command, and said, "It's like this, and it's going to take this long." It's been looking like as little as six months for a lot of the different specialties that we're looking to do but the key to this--because if you talk to someone, let's say, at NSA, it takes a longer period of time. The approach that we're looking at is part of this weapon system instead of, and I tell people, when we think about it, we're not trying to build this handcrafted car. We're not trying to develop people who are going to build and do everything with, to develop a handcrafted car. We're trying to get someone trained to be able to work on a production line who's an expert on doing their part and then over time you expand that and so, which is another reason why it's really critical for us to be able to retain these people that we'll putting into the force, so that's why we're looking at whether it's going to be the long term career development.

And the people in the Pentagon, in particular, are concerned that as we do this that before we start pulling people into this new career field we want to make sure that we've thought through the entire career path, whether it's officer, corps, enlisted, we've thought it through all the way through with the careers and we haven't set ourselves up whether you can get to, say, a mid-range NCO or even a field grade officer and we've got a real place for you to go. The good news is that everybody that looks at this says that we've started actually laying down these tracks and it really looks like it's a pretty clear-cut career path and we actually once again are hoping that by this fall that we'll be able to build up recruiters and say we're looking for these kinds of people.

Q: I'm starting a little bit to understand in a more traditional warfighting sense what

cyber means and a lot of what you talked about now and other occasions to me relates a lot to preserving comm. and C2 and ISR more generally. I want to give you three examples, and if you tell me which of them or all of them fit into future cyber--and one would be something (inaudible) with a JTAC, Predator, Rover. Another one would be a bomber using defensive ECM. And for a third one, let's assume everything gets fixed, the comm. architecture and you have an F-22 attacking a new target using TTNT. Are there cyber elements to these; are these cyber attacks, are they not? Where do you draw the lines?

A: Well, since there's cyber elements in all three of those but the--we're actually taking about the electronic protection of a bomber, we wouldn't typically think of that as a cyber mission. That's an organic platform protect the bomber. The other two, you know, the Predator, Rover, JTAC, and taking up the new TTNT tying into it for a time-sensitive charge, those are clearly the types of things that we're talking about from when we talk about a cross-domain ops. In fact, I start talking about generality, when we look at this thing, there's a, we talk about, one part of our mission is, we call expeditionary cyber (inaudible). It's this connectivity--we have to be able to go, we're a global air force, we have to go operate anywhere on the globe so that's a key piece and I really talk about that quite a bit when I was talking with you.

Then there's the defense piece, which is achieving this cyber superiority, attain the cyber superiority. There is the attack piece, if you will, which we call the counter cyber operation, which would be typical or parallel to an air superiority counterair type of operation. And then there's this, what we'd call cross-domain or counterdomain operations which you're referring to right now, which is where we are integrating cyber with air and space to achieve effects. So when we are working with a JTAC, and a Predator, and a Rover, that is a cross-domain effect. We're integrating these different domains together using cyber to do that. When you talk about the TTNT and the F-22, the (inaudible) some type of combo in that little system. And once again that's deemed as a cross-domain connectivity piece.

The counterdomain piece is where we would try to get an adversary's (inaudible) and when you look at that, that whole, particularly for the Air Force that whole (inaudible) cyber is what gives it the velocity so the better your cyber is, the quickly you can do decision-making, you can create effects. If you were to degrade it it slows you down if you take the way for us and you can't operate anymore so we thought that we had a counterdomain effect, which you talk about attacking an adversary's (inaudible) by going after the sensors itself, which can be electromagnetic or electronic attack that gets the sensor--that would be a piece of what we would do. It could be actually going against the databases and dividing the situational awareness that in some ways that you can look it it could be, it's like IO, and in some cases where you would actually go in and say, change the data or do something to modify the data. But any type of operation where we

can alter or affect situational awareness we want to be able to get into the battle management system, we want to slow down decisions (inaudible).

By the way everything I talk about we're trying to do with an adversary we're trying to defend for ourselves. So we want to be able to take away the rapid decision-making capability of an adversary and then finally, we talk about achieving effects. We want to be able to, where you have any type of a network warfighting system, we want to develop ways to use the electromagnetic spectrum to take those out. So that's where we've looked at either going after the physical infrastructure that supports it, you go after (inaudible) apertures, anything that radiates or receives has an aperture as an antenna, and every aperture, there's a place for electromagnetic energy to go after, so we somewhat do this already, I mean think of what we do with an EC-130, for example, Compass Call. We do a lot of this already. We're trying to refine this to where we take what we've been doing with electronic attack and combine it with network warfare type of techniques and see if we can't achieve greater effects against an adversary's systems. As we look at this we're saying, anything we can do to someone else, and potentially could happen to us, and so we have to make sure that we defend those systems and that includes in some cases what you might call (inaudible) directed energy, for example, could have an impact on our hardware, particularly where our chips are formed, so we have to make sure that we are not the victim of these advances in directed energy, network warfare, electronic attack. We think we're way ahead of everyone else, but people are trying to catch up.

Q: So it can be kinetic or nonkinetic effects?

A: Exactly. That's right, if you go after the physical infrastructure that supports what you do with cyber. As a matter of fact, I tell people, unlike my fighter pilot brothers, I said, you know, when you go out to fly, you don't have to worry about whether there's going to be error there. The electromagnetic spectrum's always there, but cyberspace is really where you've taken this electromagnetic spectrum and put it in a form that you can operate on, so it takes these electronic systems to create it, so you know, first thing that we have to do to have some type of an operation cyberspace is you have to create it, so we have to make sure that we've done that. All that physical infrastructure can be taken out either kinetically or non-kinetically. And I tell people I used to have a bit of a joke I'd say, here's computer network attack, and I'd show a little Pacman going across the screen. I'd say, that's one way to do it--here is the way that brings joy to every fighter pilot's heart and it's the same computer and you see it (inaudible) the disk (Laughter). And I say, that is computer network attack.

Q: (Inaudible). Get these people to accept this change (cultural change)...

A: That is an excellent question. It's actually a very good STRATCOM question--it actually affects my STRATCOM in even more in some ways than it does my current, you

know, cyber job, if you will--because Gen. Cartwright will have been a big proponent of information sharing, when you look at the things that STRATCOM has done (inaudible) to his command. There's been a lot of emphasis on trying to get information sharing across the combatant commands and across the services, so he's a big proponent and my job as the joint force component commander of global strike and integration, which he knows I have to take a deep breath if I can say it because it's such a long name, is the integration piece is the last thing that comes up and it's probably where the priority is. And this integration requires a lot of information sharing. It's not just data sharing but information sharing.

The culture piece of this is there's a couple of factors that were involved--one is that for the longest time in the military I've always had this idea that you'd have to protect information--it's a security thing, it was always we talked about a need-to-know. Now we can talk about trying to move from this culture of need-to-know, which is an inculcated for everyone that's been in every service and every agency for years. The first thing they can tell you was, you know, it's not enough that you have a security plans, you have to prove that you have a need-to-know, and now all of a sudden, forget all those things that we've been telling you from the time you entered the service, we really want you to share all this information, and people look at you like you came from another planet. So that's the kind of cultural change that we're talking about. So the sharing piece, because we so much emphasize a completely different approach to this in the past, it really has been difficult because it's not natural for us.

The second part of it has to do with as we've operated whether as a service or as an agency or as a COCOM, we've tended to think that we create this information and it's almost like an intellectual property right that comes with this and so the cultural piece that's required here is to convince everyone that really this information, even though you created it, it really belongs to the nation because you're working for the nation, not for yourself, so it's really not your information, it's the nation's information. And if that would help someone else to defend the nation then you really ought to share it. In principle, everyone agrees with this, but the problem is that all the systems that we developed early have been designed to protect information from being shared, largely because we didn't want our adversaries to get it. So that's what, when we talk about this cultural shift, that's where the complexity comes in. We really designed our whole way of doing business to be completely different, so that's where the challenge comes.

But we made great progress--you have to give one heck of a lot of credit to Gen. Cartwright and OSD, Mr. John Grimes, and people that have worked there and have really been pushing this need to share information and where you can see the progress is really some of the things that have been going on with STRATCOM now--they have, it's called a SKI-web; SKI stands for Strategic Knowledge Information. This thing's set up with all the COCOMS and the other COCOMs have really bought into this and

STRATCOM said, this is not our information system, we have set this thing up so that all of you can share information, and basically, anyone, it's a blog site basically, classified blog site. It currently is set up to exchange information, by the way, with the Brits and the Australians and looking at ways to expand that because we've recognized that you have to be able to share with your coalition partners. It's set up with other agencies as well, so obviously, NSA, DIA, because their actions in a sense associate with STRATCOM through these other joint force component commands; tremendous information sharing that's going on there, so that it's working. Now within the Air Force piece the way that we want to share the info is through our air operation center. We have an air operation center in every theater of operation and we have great situational awareness of that theater, and now what we recognize is that (inaudible) cyber and also with the cruise missiles and with theater ballistic missiles, you can have threat to cross these AORs. We're trying to use these AOCs by connecting them. Gen. Cartwright is advocating this to link with these AOCs so that there are no seams across the AORs and there's a lot of data-sharing that goes on there; we're making pretty good progress.

Q: General, you mentioned several times the need for the US to maintain its pre-eminence in cyber warfare, and you mentioned AETC and other places like that. How different is this than maintaining our pre-eminence in bombers and in fighters given the way information oozes, given the networking, I mean, is it the same way to maintain the pre-eminence? And would it require something different, or is it basically you're always trying chase your tail, you're just going to be able to maintain a little bit of edge?

A: In some ways it's similar to the pre-eminence we're looking for in air and space but the realities you've heard people several times say that when you go into a fight, we're not interested in making it a fair fight. We want to go in and knock 'em out on a first round. People might be upset, they say, you paid for a big fight here and you came in, gave him one punch and he was down. We're perfectly content to do that because, quite frankly what you'd really like to do in this business is not have to have a fight. So you'd like your adversaries to know that there's really no reason to try to take you on because you have such capability that it's not going to work. And this goes to the concept of deterrence or dissuasion and (inaudible) like to promote that but now when you talk about this we as a nation still are really the leader, say, in information technologies. I mean, there's a lot of people getting into this but this nation really had that leadership--other people are kind of exploiting our open society and those types of things, so what we're trying to do is take our intellectual, again, the great intellect of this nation--not just the Air Force, but the intellect of the nation and our technological might and the fact that we're able to integrate these things together--and put that in a way that we can use to defend the nation, particularly from our standpoint, one of these things, we're not trying to solve world hunger, we're trying to make sure that our ability to conduct military operations and to interact not only as a military force but with other agencies and government, is not impeded because we can't, we don't have the connectivity that

allows that to happen.

So is there going to be information oozing out, if you will--sure, because this network is huge and there's a lot of information, but again this is less about information operations and it's more about really ensuring that we can continue to function as a superpower and put all the capabilities of the nation, of the military and diplomatic, traditional, economic, put these things together and really--there's a briefing of, people saying you're trying to start a Cold War by talking about deterrence. The Cold War wasn't about deterrence; deterrence was a way that we acted during the Cold War. Deterrence is not a bad thing, Sun Tzu talked about deterrence, he didn't use that word but a couple of thousand years ago when he said that it was better to defeat your adversary without a fight. And that's what we'd really like to do, we would like to have our potential adversaries say, you know, it's not worth taking the United States on because they are so much better at us in air and space and cyberspace and they cross our capabilities that we're just not even trying to fight with them.

Q: Where do things stand doctrine-wise, particularly given computer network attack and non-kinetic and how related everything is in that world? What are fair targets? Obviously military infrastructure, what about civilian infrastructure--and only during hostilities or peacetime or pre-emptively?

A: That's interesting when you specifically narrow in on the information ops piece; like everything else, we're exploring the rules of engagement and when we think about this a lot of times right away we start looking at this in a peacetime context where what you can do in peacetime is quite constrained as opposed to what your rules of engagement might be when you're actually engaged in some time of operation, so the answer is that it's going to be situation-specific, and the rules of engagement are going to be determined by the Secretary of Defense and by the President, for a given situation they say these are your operating lanes that you can work in, but (inaudible) just as you would do with any type of an air effect or space effect we are looking to provide very precise effects. So the idea is we want to minimize collateral damage so will a civilian target be a legitimate target--if it's purely civilian target, generally from all the laws of armed conflict, you don't go after civilian targets. So you try to minimize the impact and the same thing for cyber you're going to try to minimize any type of effects that you have that would affect a civilian.

Q: (Inaudible) with collateral damage is not permanent so does that push back the availability of that tool frame?

A: Well, when you actually look at, let's say, one good thing, when we start talking about there's a precision thing, and when we, one nice thing about computer network attack is that it tends to be very precise and so when we, this idea that we're going to have the

collateral damage because it's going to affect the civilian infrastructure. If we go after a military target, we're going to go after a specific piece of equipment that we're looking for, but again, it's kind of interesting--a lot of the talk, thoughts about cyber warfare really focus on computer network attack, whereas, let me tell you that our big focus is on the use of cyber for warfighting operations, so we're less worried about that computer that's on someone's desk as we are a warfighting system, integrated air defense system, for example, command and control systems, systems that pose a threat to the US that we might take out. (inaudible) take away the situational awareness that they need to operate the system, actually we go after the system itself, so it's not to say we're not going to be involved in what has traditionally thought of as computer network attacks; that we're working now with joint force component command network warfare which is (inaudible) my title (Laughter.) and we're actually doing, we're doing operations with them right now and those are the exact thing we're talking about--we're going after specific computers working with net warfare, but that's a small piece of this larger capability we're trying to develop, which is really about an integration of effects across not only the military but our capabilities as a nation.

Q: You still do airplanes and missiles, right? (Laughter.) Can you tell us about the thinking behind taking down the ACM-3 and however many of the ALCMs you're going to take in and whether that ties in with your desire to burden the Air Force of a certain number of B-52s?

A: The ACM piece is actually unrelated to the B-52s right upfront. When you look at, we have these weapon systems to support war plan--in this case, it's a war plan we hope we don't need to use of course, and we still maintain a viable triad. The ACMs, although a newer cruise missile posed some interesting challenges in terms of how we operated them, and we actually had greater flexibility in terms of how we could use the ALCMs, and so-- (Question inaudible). No, it's mostly a maintenance problem--they were difficult to maintain.

The other thing, by the way, they could only be carried externally and so there's a fuel issue that goes when you have to carry these things externally. In fact, when you load the things up the fuel required to carry the things is about 20 percent above what it would take for the same distance to carry it internally, but the fuel wasn't a big driver. The big driver was really the maintainability and the reality that through a lot of other improvements and the way that these systems are going to be used, the ALCM actually provided a better platform for what the STRATCOM planners were looking for. So this was done to really satisfy the STRATCOM mission needs.

("So stealth was of a diminishing importance?") Well, part of the problem was that stealth is always as important and that's one of the ways--you have to go back, and it's an effects thing--stealth is there to improve your access, so you don't need stealth to

have the effect on the target, you have to have stealth so you can get to the target and because of the way that these things are now being employed, we have other ways to, which I can't talk about here, we have other ways to get those ALCMs to the target. And the benefits that we're getting in terms of the--this is a first generation stealth--and if you think about where we've gone from the F-117 to the B-2 and now we're at the F-22 in terms of what we could do with stealth. When you think of all the problems in terms of maintainability of the earlier stealth, this is a very--maintaining the stealth on these things was very difficult to do, so that's why we look at other ways to provide the access that you need, which we've been able to do.

Q: What about the B-52s?

A: I just said it's unrelated to the number of B-52s.

Q: How big a threat specifically is cyber attack terrorists?

A: It depends on what you mean by--cyber attacks and terrorists against our warfighting systems is; we're actually, from a warfighting standpoint, these days I think we're more concerned about nation-state attacks on warfighting systems, because you're talking I think about cyber attacks that might affect other parts of the nation, for example, take down (inaudible). Like anything else, to be really good at this, you can have a backyard capability--if you don't have someone that's supporting you--if you have a terrorist that's kind of operating on their own they're going to have less capability than if they have nation-state sponsorship, because to really get to some of the advanced capabilities that you're going to need to have a serious effect on the nation, you're going to have to have some pretty sophisticated techniques.

Unfortunately as you know, most terrorist organizations do get some kind of nation-state sponsorship so this is a realistic problem, but I guess what I'm trying to tell you is that the terrorists would be using--the tools that they'd be using are going to largely, likely be provided by some nation-state that's working to--or the other thing is organized crimes. You need some kind of big organization that really does this thing as a business (inaudible) to be able to do this. Now the reality is that we in the United States we do a lot of things not only in the military but across our systems. When I go to (inaudible) looking for ways to prove how we do business. We actually go to places like the bank and industry financial, some of these other systems, to see how they do it because they've done some great work in this area, and I'm really impressed when I go to some of our businesses that really depend on cyber just like we depend on it for warfighting, they know they depend on it as well and they've done a lot of really smart things to shore up, you know, what they do with their protection of their network capabilities. So to seriously disrupt, you're not going to do this with a teenage hacker type capability--it's going to have to be something that's pretty sophisticated.

Q: Question about technological advancements they're looking for and things like that and also about how much money for investment in this part of advancements?

A: I can give you some specifics on both of this--what we're trying to do in '08 and '09 is we're trying to accelerate the programs that are tied to survivability of the Air Force portion of the global information grid, so there's a whole host of programs it's primarily tied to--it's called CITS Block 30, Combat Information Transport System Block 30. This is a system that is reducing our exposure to the commercial Internet. It's providing us much greater situational awareness in terms of being able to track the traffic on our networks because that's really the key to how to protect the networks is to monitor what's going on and we have this program in place to do this. We're trying to accelerate that program because by accelerating this; the word I use is survivable it's not secure; it's going to be secure. What we realize is that it's not enough to have a secure network, it's got to be a survivable network because people are going to shoot at you in a war. People are going to attack your networks so we have to make sure that our networks are survivable so we're talking about shifting money and it's quite a bit of money, but it's within the current program.

What we're trying to do is take money that was currently provisioned for doing new information technology and say, well we could spend a lot of this on some tech refresh, but it would be better spent if we put it into the survivability because it would actually then reduce the costs (inaudible) the tech refresh. The exact figures of the program we're still trying to sort out but it's not small. (Question inaudible). Some things we're trying to do with the CITS Block 30, for example, are the in the range of half a billion dollars, so once again, it's money that's already in the budget that's being moved around to support that, and in terms of the software we're looking at, in fact we started this year putting money into a couple of different programs--one's called application assurance. Those are actually done at Gunter--(inaudible) electronic support group and what this is, we are testing software, both commercial off-the-shelf software and government purchased software and there are tools you can use to cut through the software to expose vulnerabilities before the hackers find them ,quite frankly, and then once you know what the vulnerabilities are you can protect against the vulnerabilities by putting wrappers around either of the application or the database. By wrapper, it's like a portal--you can't go directly to the database you got to go through the portal. The portal won't let the things we found would be able to use that vulnerability to get through. This year, it's a start of \$4.5 million this year--start to work in that area and they're going after some of our combat support systems to protect those particular systems. And we're looking, database wrappers and also database encryption--we expect this year to be letting up a contract, and once again it's coming out in Gunter, by the way, for database encryption that they'll use across the Air Force for our warfighting systems, it'll automatically (inaudible) encrypt everything we're doing. It's just much more difficult

for someone to fool with your system when the data's encrypted. We're looking to put that in place, so that's all happening this year.

Q: (Question inaudible)

A: I probably wouldn't want to tell you what our greatest vulnerability was, but China has put a lot of resources into this business, so it's hard to say. There are so many nation-states that are working on this--it's hard to pick your favorite one, but China (inaudible)--they actually have doctrine, that's public doctrine that says that there are five domains in which you have to dominate to be successful; they're air, land, sea, and space, and they won't say cyberspace, they'll say the electromagnetic spectrum. That's in their doctrine, they're very public about it and they said that we intend to develop the capabilities to dominate those five battlespace, those five domains. And they're the only nation that's been quite that blatant about saying, we're looking to do that. They're not our only peer adversary.

Our biggest vulnerability, quite frankly, I can tell you this, is because it's tied to something we're trying to fix, and it actually affects everyone in the nation, and that is, we think we live in a safe neighborhood and you don't need to lock your door. That's our greatest vulnerability is that we fail to recognize just what the threat is. So we have a program that we started in the Air Force, we call it our cyber safety program, and it uses, in fact we have a safety office helping lead this into (inaudible), it's called operational risk management to improve our safety, (inaudible) ground safety. I said, you know, those same techniques that work to prove the safety of our cyber and we also tell our airmen that in this program that basically every airman, if you would go into the AOR now everyone carries a side arm or a rifle because that's called defense in depth, so for our airmen we're trying to expose them to the fact that they are our best defense because people don't realize most attacks that occur on our system don't occur because of some sophisticated hacker being able to break through a firewall or do something like that. It's usually social engineering--the easiest way to attack a system is to get someone to do it from the inside. We call it the insider trap but it's not a spy because people just aren't conscious of things that they do that really expose the system. We are working with all of our airmen to make sure they understand these potential threats, and in fact, you see the same thing happening--(inaudible) I watched the Vista commercials, and they keep poking fun at the guy that's getting all the warnings, but the reality is that the reason those warnings come up is to remind the people, hey, do you really want to do this, you are exposing yourself to a threat, do you really know where this came from?

So our biggest threat is the insider threat; it's not a spy, it's making sure that people recognize that this is not a safe neighborhood. We think it is, whether you're at home working on your desktop or you're in the office or you're working on a combat system, you can inadvertently be the person that takes that system down because it can be as

simple as a vendor giving you a CD, for example: hey, I got some great demo software for you--stick it in there, it does an auto-run, next thing you know your system's infected, and they're back behind your firewall and they're just having a ball.

Q: (Inaudible.) How much progress have they made?

A: That's really hard to--it's actually really hard for me to make an estimate in terms of--it's hard for me to put it into context. We know that there's a lot of activity from China. You know who could give you a really good feel for this--you can go to talk someone like Akamai--are you familiar with Akamai? It's a civilian company. When you go to a Website, you go to download something, you think you're going to a website you don't really go to a website, you actually go to an Akamai server most likely, and that's where you download. Akamai tracks very well where these threats are coming to their, against their servers, and they actually track which countries, because they know where the IP, the Internet protocol address, are coming from. They can give you a pretty good indication of where these scans, I guess, are coming from, but from what I've seen, China is primarily at this point, not interested so much in attack as they are, like everyone else, they're using the Internet to pull data information either for, which affects our companies because its proprietary information because they now don't have to develop this. As a matter of fact, I'd say that a lot of this is really economically-based. When you look at the kind of philosophy that the Chinese have, (inaudible) Sun Tzu came from, they're actually doing this in a way where they can be dominant without having to have a fight. So, they're very good at it they put a lot of resources into it, but in terms of a way to quantify that, I'm having a hard time figuring out a way that I could quantify it for you.

Q: (Inaudible) Question about SECAF going to Congress--do you need some money or some legislative authority?

A: The people in the Pentagon are the ones that are working on this. Typically, whenever you stand up a new command it's within the Title 10 authorities of a service, but there's notification, it's more of a notification process that's involved. I have to admit I'm not the expert on this, so I just know that when we start talking about timelines, we talk to people who do this, they say, you know we have to do this process with OSD and it's all done. I hate to push this off, they give me enough things to do, when someone says, I've got it, I say thank God you took it. So within the Pentagon, there's processes to work this, and so OSD (inaudible) the Department of Defense there's notifications and then Congress as well.

Q: (Inaudible).

A: Well no, I don't know what that time is going to be. My job, my task was to establish

the on-ramp and what I've told the Chief and the Secretary is that I'm working aggressively so that I have everything in the on-ramp, everything ready by the end of the summer. Then they will have to determine what the right timing's going to be.

Q: Question about updates on long-range strike, what you think will be the best with regards to timelines.

A: I am a bomber guy, by the way, so I'm pretty excited about the long-range strike, the next-generation bomber. And this thing grew at a fast pace, the Chief and Secretary committed to having this thing with an IOC in 2018. Once again, when you're talking about a bomber, one thing you have to look at is, what is it that you want a bomber for? And you want something that can go long ranges, great distances--you want it to be able to have access. So part of this is a, you want to be able to operate globally, get access, and the other thing you look for with the bomber is persistence, so as the Air Force has been pursuing this, they say what we really want to do is expand our capabilities in this area and be able to deal with some, you might call anti-access, so the reason that this thing is doable in 2018 is that the technologies exist.

Some people say, why not go to the next thing, hypersonics, and advanced propulsion, and other things. Well, in reality those technologies aren't quite ready, and that's why the bomber they're looking at for 2035 we're looking at those technologies, but for 2018, we have technologies that we can exploit quickly. The F-22's stealth, for example, maneuverability, a lot of things are involved with that. A number of other programs, and you're familiar with some, some maybe (inaudible), some never made it out of the (inaudible) but a lot of technology development that can be plowed back into this airplane and I was not part of the study but as it turns out, to be able to do the types of things that they want to do with today's technology that drives you to a subsonic bomber and achieves what we're looking for. We're an effects-based Air Force, we look for effects, and access we'll get, long range, we'll get, persistence, we'll get, and the ability to work with advanced munitions, we'll get. And when you talk to the Chief about the next generation bomber, he lights up. He's so excited about it, so he is the Air Force's biggest proponent for the next generation bomber and when you have that kind of advocacy I'm fairly confident that we'll see; in fact, I told him the other day that I wanted to be the first one to fly it--and he said, I have this funny feeling that you'd be retired by then (Laughter), so I said, darn.

Q: (Inaudible.) What about the B-2? It's a stealthy aircraft, it's got really good range--?

A: What's interesting is, I was talking about that earlier with the ECM, first generation, second generation, third generation stealth, B-2 is a second generation stealth--we are so much further ahead in terms of what we can do with stealth now that you'd be coming after me for (inaudible) to spend more money to develop--the F-22 is so good and the

technology, incorporating those types of technologies, some of the other technologies that we have, particularly when you're talking about 10 years from now, it's the same thing. Why was the Air Force so adamant about wanting to get JSF and now the F-35 and the F-22--it's because you want to have the very best in cutting-edge technology so that we have--the B-2 is a great platform that's going to continue to be a great platform for a long time, but the technologies we have we can plow into this next bomber will (inaudible) people's eyes when this thing comes out. It's phenomenal.

Q: Following up on your comment that we know there's a lot of activity from China, can you clarify what exactly you're talking about in terms of that activity, and what other countries are posing any potential threat in cyberspace?

A: An easy one. Well, first of all, how do we know that it's China, because the Internet protocol address you can track them back to China. And the activity, as I mentioned earlier, it's really, for the most part what we've seen is industrial espionage in large measure--or even when they go against our networks that's what they're looking for is system information, that type of thing. So it's things that you can build systems. In other words, if you think about it, you can spend 10 years doing the introductory research to develop some new capability or, shoot, if someone will give it to you by leaving it laying on the table, if you will, which is why things like encryption, they get to be so important. Any country that you can think of as a potential adversary is on scanning our networks, so pick an adversary--("How about Iran, North Korea, Russia?") Actually, everyone but North Korea--we've concluded that there must be only one laptop in all the country, and that guy's not allowed to scan (Laughter.) I'm serious, for all the things we say about North Korea, that's one thing--they don't pose a cyber threat. Every other country, you name it, every country is involved scanning our networks.

END TEXT