

Department of Defense Bloggers Roundtable With Lieutenant General Susan Lawrence (U.S. Army), Chief Information Officer (CIO/G-6); Lieutenant General Rhett Hernandez (U.S. Army), Commanding General, U.S. Army Cyber Command; Major General Alan Lynn (U.S. Army), Commander, Fort Gordon, Georgia, and U.S. Army Signal Center of Excellence; and Major General Jennifer Napper (U.S. Army), Commander, Network Enterprise Technology Command (NETCOM)/9th Signal Command, Fort Huachuca, Ariz. Moderator: Margaret McBride, Spokesperson, Army CIO/G-6 Subject: Network of 2020 Vision and the future of Army Cyberforces. The LandWarNet Conference in Tampa, Florida Time: 11:06 a.m. EDT Date: Wednesday, August 24 , 2011

-----  
Copyright (c) 2011 by Federal News Service, Inc., Ste. 500 1000 Vermont Avenue, NW, Washington, DC 20005, USA. Federal News Service is a private firm not affiliated with the federal government. No portion of this transcript may be copied, sold or retransmitted without the written authority of Federal News Service, Inc. Copyright is not claimed as to any part of the original work prepared by a United States government officer or employee as a part of that person's official duties. For information on subscribing to the FNS Internet Service, please visit <http://www.fednews.com> or call (202) 347-1400  
-----

(Note: Please refer to [www.dod.mil](http://www.dod.mil) for more information.)

LIEUTENANT GENERAL RHETT HERNANDEZ: So, I'm Lieutenant General Rhett Hernandez, commanding general of Army Cyber Command of the United States Army. And I really want to spend a couple of minutes telling you who we are and what we've been doing for about the last 10 months, and a little bit about the way ahead. As we work to train, organize and equip around cyberspace as a domain, we must ensure we maintain the freedom to operate. And as you all know, and we've talked about it each day so far, the threat's real, growing, sophisticated and evolving. Recognizing the need to operate and defend against cyber threats and the importance of enabling mission command, the Army activated Army Cyber Command, 2nd United States Army, on 1 October, 2010. The command provides unprecedented unity of effort and full-spectrum cyberspace operations, and is a global command with more than 21,000 soldiers and civilians serving worldwide.

Our mission is to direct and conduct network operations in defense of all Army networks; when directed, conduct cyberspace operations in support of full-spectrum operations, to ensure U.S. allies -- (audio break) -- of action -- (audio break) -- cyberspace, and deny the same to our adversaries. We serve as the cyberspace component for the Army and coordinate information operations for the Army. We're the service component to the U.S. Cyber Command.

With this mission, a few highlights on how we're organized. We have a major headquarters based at Fort Belvoir and Fort Meade, and three supporting commands: NETCOM/9th Signal Command, with Major General Napper here today; and Intelligence and Security Command and Information Operations Command. Our operations center directs our mission and --

(inaudible) -- is our Center of Excellence. Additionally, we're growing a cyberbrigadecyber brigade to serve as our operational arm for full-spectrum capabilities.

In the last year, we've been pretty busy. As you consider we've started from scratch, we've accomplished some major objectives that I'd like to highlight. First and foremost, we've established a high level of integrated systems with Cyber Command and our fellow service cyber components. We have an operational focus with an unprecedented unity of effort in operating and defending all Army networks globally in the 21st century; heavily engaged in operational planning with U.S. Cyber Command, contributing with cyberspace planners, and are focusing our efforts on cyberspace operations -- (audio break).

Just -- I believe we have really planned and achieved cyber integration into major exercises. I'm excited that we've established the Army's Cyber Proponent for force development work. Additionally, we've conducted a comprehensive Army cyberspace assessment, leading to our work on an Army cyber 2020 strategic plan.

While our mission is clear, so, too, is our vision for Army cyber 2020 starting to take shape. I envision a professional team of elite, trusted, precise, disciplined cyberwarriorscyber warriors defending Army networks; when directed, able to provide dominant full-spectrum cyber effects, enabling mission command and ensuring a decisive global advantage.

The work on our strategic plan is intended to help achieve our vision, and it, too, is gaining clarity. We have three major lines of effort to guide our work: First, operationalize cyber; second, grow army cyber capacity and capability; and third, recruit, develop and retain the right cyber warrior force.

The final point I'd like to make is that for a command built around technology, it's important to remember our most valuable asset: our people. They're the centerpiece to our work. Our soldiers and civilians will determine our success and ensure that we remain second to none.

I want to thank you for those few brief comments, and I look forward to your questions.

LIEUTENANT GENERAL SUSAN LAWRENCE: Thank you.

Well, good morning. I hope you all, especially those that are here in the room are enjoying the conference -- I think we really made a difference today in bringing different type of speakers in to motivate us to think about the different things innovatively. And we just now demonstrated to you what a disruption is in a cyber environment -- (laughter) -- by bringing in these callers, as they talk about the definition of cyber. There you go.

Well, for those that heard me speak yesterday, I've taken the first four months of my time as the CIO/G-6 to look at where we need to

focus, what should the vision be. And I discussed the need to look at the Network 2020: over the next three POMs, where we want to be to support what is going to be a smaller but much more capable Army for us. And that is ensuring that we're the -- remain the most powerful land force in the world as we go through this.

So the vision is "The Network of 2020: Powering America's Army," as we look at this. And why is this important? One of the forcing functions of keeping us connected globally is the things we've been working on for the last few years, and that's been the base realignment and closures. We're now an 80-percent CONUS-based Army. And what that means is we have to have the network empower that CONUS-based Army so that they can be better-trained, train as they fight; the ability to deploy with little to no notice into any austere environment, but be connected to their mission command applications. And that's what we're going to work for. And so our bumper sticker on that is "always networked, always on," as we do it. You've seen -- many of you've been at my other presentations as I talk about the connection. And that is the first step that we're doing, the single identity: that soldier that can take his CAC card or her CAC card and go anywhere in the world, put it into a government computer and have immediate access to their information, because at the end of the day that's what it's all about -- the data -- as we work through it. So whether the soldier is sitting at home or TDY or at their post camp and station or deployed in Iraq, Afghanistan, Libya, Syria -- in any austere environment, they can connect to the information.

And we're finishing out this year our last two Regional Hub Nodes. And so what that means -- the last two are in Camp Roberts, California, and Guam. And so an individual could take a suitcase satellite terminal with them, and connect to any two locations around the world and immediately be connected to the Global Network Enterprise and have access to their information. And that's what's going to be key and the power of what we're going to be able to do as we work through that.

And we talk about that cloud in the middle. And this is where the hard work is. This is where we're really having to roll our sleeves up. And that is cleaning up our applications; what are the relevant applications; what services are needed by our men and women serving; and the data. And so you heard a little bit from Admiral McRaven today. When we talk about data, where is it, how's it tagged, how do I get to it, how will I recognize it? And that's what I -- and trust it -- and that's the other element that we bring into -- in our partnership with cyber operations: that's trusted information, as we're working through it.

And so we're looking at four imperatives as we build this network out. And the first and most important one is that we're going to build a single, secure, standard-based network. That is, if you're serving in Europe or the Pacific or continental United States, it is the same network. And today the problem we have is -- you saw from Ms. Takai, if you were in her presentation, you know, 15,000 different networks out there. You can't share information across those

environments. It has to be a single environment in which to do it. And that's what we're going to be moving towards as we work through it.

Enabling the global collaboration: How are we going to command and control? How are we going to fight across this network as we do it? And yet, that is the ability -- again you heard from Admiral McRaven, the ability to reach a web portal or the data that they need in a collaborative environment.

And you're going to hear from Mr. Chambers tomorrow and I -- he spoke last week, and the thing that he talks about is videoing. I mean, that is the future. Everybody wants full-motion video.

So key is cleaning up this network, because that's going to take a little bit more bandwidth. And that is -- that -- you think about our soldiers deployed. Video -- they're skypeing home to see their children and their significant others as they're going through it. And so that's the network that we've got to enable, and those are the things we're looking at.

So as I look across the three POMs, what are the immediate things that we need to do today to get that foundational environment to ensure the third imperative? And that is access at the point of the need. Whether you're in a training environment or you're in an operational environment, touching the network is what we're going to be able to do.

And that's the last imperative -- capable, reliable and trusted -- and that is key). I was asked recently in a discussion -- they said: Well, what's your -- what's the hardest -- what's your biggest impediment to achieving this? And I said it has to be the culture. It is the environment if I can't touch it myself, if I don't own it, I don't trust it.

And I give the example, when somebody says that to me -- you know, especially some of our senior folks, who said: I can have someone be responsive to me within 10 minutes.

And I said: Well, OK. I said: That's fair, and that can go into a license agreement.

And we'll have Jennifer talk a little bit about how we're going to work through these things.

But I said: Well, who's your Internet service provider? Is it Yahoo or -- you know, Gmail or AOL?

And they'll say: AOL.

I said: Well, great. I said: Before you log in at night, do you call AOL and say: Where's my server? I am -- I don't trust you. I am not going to use you unless I can -- I can touch my server. Or do you flip open your cellphone and call Verizon and say: Where's the power? I really cannot trust you unless I know where that power is.

And so intuitively we know what we're doing is right and headed in the right direction. It's just working through the culture of the trust as we do this.

So again, thanks for being here and sharing with us during this time.

MAJOR GENERAL JENNIFER NAPPER: Good morning. I'm Jennifer Napper. I command Network Enterprise Technology Command, 9th Signal Command. There are some little pamphlets that have all the bits and bytes of what I've probably going to say in front of you.

We are the operational arm of building, operating, maintaining and defending a network for the Army. So in the short synopsis, I'd say our job is to execute the vision of the CIO in accordance with the orders from Army Cyber Command, OK, so that's kind of the way we work.

It's an exciting time for us. We're in the middle of implementing all the global network enterprise initiatives that General Sorenson and now General Lawrence have been talking about for about three years. And so any of the initiatives that you've heard about, like Enterprise Email or data center consolidation or collapsing down the domain controls in our active directory or any of the others, that is our number-one focus as we move out.

The second focus we have this year is transforming the way we deliver the capabilities on every post -- (inaudible) -- station globally. As you heard General Lawrence say, we're getting at this as an enterprise approach. We've got -- built together a process we're calling Army Baseline IT Services, ABITS, by which we can identify what kind of capabilities they need in the posts, camps and stations; how -- what are the resources necessary to deliver that; and then get that down to one enterprise, as opposed to the multiple -- (inaudible) -- 15,000 networks and how many other commands providing that today.

That's a -- that's a really exciting new line of effort for us this year. You'll probably hear a lot more about it over the year.

And our third focus, similar to what you heard from both of the other generals on my left, is people. We understand that there's a finite number of folks in this country with the right skills and the right clearance or clearability to really help us in our mission set. And unfortunately, a large number of our folks have been with us for 20 or 30 years and are at that point -- (inaudible); about 34 percent in the next five years are retirement-eligible in our population. And that is -- really putting the pressure on us to look differently at how we go out and recruit some of the young folks to come on in and help us with this business. And if we have a bumper sticker, it's that we're one team in the Army providing one network.

General Lynn.

MAJOR GENERAL ALAN LYNN: Thank you, and good morning. I'm Major General Alan Lynn. I am the commander for Fort Gordon and the Signal Center of Excellence. I also have the honor of being the 35th chief of Signal. Essentially what I do is I run the university for signal officers, noncommissioned officers, soldiers and warrant officers. We also provide the future vision for the Signal Regiment.

What I've been working on the last year is essentially a fundamental change to the Signal Corps. Our current design that we were running on was probably Desert Storm-era doctrine, where we provided support just down to the battalion level. And as you know, battalion level is just not low enough in the formation right now. So the Combined Arms Center at Fort Leavenworth took a look at what our requirements would be and they came across the mission-essential capabilities list that we needed to provide. And that included communications down to the company level and below.

There was one caveat, though. They didn't want us to grow the number of actual signal soldiers that we would have, so we had to go from battalion level down to company level and below without any growth in personnel.

So the only rheostat on that was to really take a look at the equipment set. So what we needed to do was really take a hard look at our structure, take a look at the doctrine, take a look at the training, take a look at equipment and the employment of signal forces. And so what we came up with is we need smaller, more capable teams, much like the special operations forces use, like JCSE is currently running with, smaller, more capable systems as well. So commercial standards, a lot of commercial off-the-shelf. We're even looking at some small hand-helds, including iPhones and Droids. But this will allow us to cover more area because they're smaller teams. Same number of people but smaller teams, more capable equipment; we can go further down in the force to provide support.

The other thing we're having to look at is re-looking the way we train the force, because as these systems come in, there's going to be multiple different kinds of systems a soldier will have to operate. Instead of training them to train on one box, for example, we just train a satellite operator today. Tomorrow we're going to teach them the theory of satellite, line-of-sight and tropospheric scatter. So they'll understand the theory of it. So as the boxes change -- as we go through Moore's law, the boxes will change more rapidly, they'll understand the theory of the systems, and then we just have to teach them how to operate the buttons. So the buttons piece they'll be getting from their apps, the applications that we develop. We are developing our own apps at the Signal Center of Excellence as well.

So these apps are how the soldiers like to train today. If you show them a proctor and a PowerPoint slide, they will just look at you like, what, are you kidding me? They want to have that touch and feel, that system that they can actually see it visually on a screen, plug in cables on a screen, and we're doing that at the Signal Center today. That's actually happening today. And then by the time they actually get

to the equipment, they're very familiar with it, they know how to operate it, and that's the way they like to learn.

We're also looking at virtualizing some of the training so the live -- (inaudible) -- we're going to have live training, but we'll have virtual and constructive and gaming. Folks today are interested in gaming. So if we develop this environment -- we're already working this in a number of the different centers of excellence. And a soldier goes into it -- they care about their avatar. They really care about their avatar. If they go out and they shoot OK out at the range, they shoot marksman, so that score is put into the gaming system. So if they only shoot marksman when they're out playing on the virtual gaming environment, they don't do as well as their buddies, so their buddies are yelling, hey, come on -- at their avatar, hey, come on.

And for their PT test, if they don't run as fast on their PT test, that's what we put into the game, that they can't run as fast. So they care about -- it's kind of a different way of looking at things. They care about that avatar, and if the avatar is not performing well in the gaming, then their buddies are beating them up about, hey, you need to go back and take your PT test; you need to go back and go shoot again so we can get your scores up so you're a better teammate.

And so it's a new paradigm, a new way of thinking, a new way of training, and it really is pretty exciting.

So that's what I do.

MS. MCBRIDE: OK. Well, thank you all.

And why don't we open it up now for questions for the folks in the room? Now, I think we -- it might be a good thing to check and see if we have our people on -- are the media and bloggers still on the line?

Q: Yes.

Q: Yes.

Q: Yes.

Q: Yes.

MS. MCBRIDE: OK, all right. Thank you for cutting the background noise.

OK, so we're going to start with folks in the room. Jarred Serbu, I mean --

Q: (Inaudible.)

GEN. NAPPER: Well, it's actually two parts. One is, where it's appropriate, applications of services should be -- (inaudible) -- unless they're local. And some are very specialized and need to stay local.

So the example General Lawrence was giving you about someone who wanted a 10-minute response, the way we do human resource management, those systems that they use for evaluation boards and things like that are only used at one place. So that's not going to -- it wouldn't make sense for me to host that somewhere in another country -- you know, across the country, so yes and no. Where it makes sense, the enterprise applications and services will be pulled up and that load taken off of the local net or network enterprise centers. Where it's not appropriate, we'll keep that data down. But we will consolidate these into data centers but much less of them so we can properly operate them and defend them.

Q: I mean, do you see that being significant enough if you end up needing less local IT manpower -- (inaudible)?

GEN. NAPPER: Yes, but we still need -- (inaudible) -- never forget that. And they are -- (inaudible) -- some things stay local.

Q: Thank you.

MS. MCBRIDE: Questions? Any other questions? Well, Hank (ph), do you --

Q: Well, I guess if -- I'm not sure who to ask, General Napper or Lawrence, about the consolidation -- data center consolidation, how is that coming along, where does that stand, where is it going?

GEN. LAWRENCE: Remember what I said my toughest challenge was? (Chuckles.) Culture. So we're moving out. And in fact, the Army is one of the more proactive ones in federal service. And so when you look at all the data centers across federal service, we're going to take down about 25 percent of them, for all the right reasons.

You know, one of the things that we learned during Operation Rampart Yankee is that we were operating at a very low, inefficient rate across all our servers in the Army. So this is just a no-kidding, smart thing to do. So two-fold: One is not just the physical doing the data center consolidation, but spring cleaning. We have old applications we've been maintaining for a long time.

And so as we reduce a data center or consolidate it, we are mandating that you will cut your current applications 30 to 50 percent. Now there's where you're going to get real savings -- and Jared, as you said, in the manpower. And so as we go down from 300 data centers to 75 or whatever -- and it's going to be even below that by the time we're done -- is less people obviously needed to maintain it as we're looking at it. Because we have some shortfalls in other areas, and so what we're going to do is, where we find these inefficiencies, we're going to harvest those individuals and then put them where we're short -- they will pay our own bills, at the end of the day.

And what is going to be key is, as the secretary of defense said on the front page of The Wall Street Journal, is that we're going to save a half a billion dollars at the end of doing this. And what is critical,

if we don't capture those savings today, they will just go away; they'll just be absorbed somewhere.

So we have a closure report that we're doing with each of our data centers. And we say, OK, how many people were working in there? How many contracts did you have? What were your O&M expenditures? What was your hardware? And they have to fill this report out to cut back into what we have built for the dashboard so then we can tell them where the (disposition ?) of those people and those dollars so that we can recapitalize them into what we're doing and some of the initiatives that I talked about. Well, the first set of reports that came in said, no, no, no, NA (ph), NA (ph). (Laughs.) I said, OK, you had no people running it and it didn't cost you anything, so now I'm moving everything to your data center. (Laughs.) So it's -- you know, that's the hard part.

But we're just doing the first step right now, and we're getting our procedures down. And this is going to be a real win for our service as we -- as we get moving on this.

MS. MCBRIDE: (Inaudible.)

Q: Yes, I was interested in the cost savings achieved by using Enterprise Email. There was some literature that, you know, savings for -- (inaudible) -- be about \$500 million.

GEN. LAWRENCE: Right, right.

Q: How did you come up with that figure?

GEN. LAWRENCE: Yeah, it's a combination between the data center consolidations and the Enterprise Email. And so what we did is we were working our business case analysis. We computed what it costs to have a soldier have an email account today. And if it's -- and it was very expensive. It was over \$125 just for a basic email account. And so today by going through a managed service and doing the consolidations, that same account now is costing us about \$34. And so that's where the huge savings are.

Today we have multiple help desks on installations managing their post, camp and station email. In the future we're going to have an Enterprise service desk that you're -- just like we've stood up in Europe when I was in command there. So anywhere in Europe, you could pick up the phone and dial 119. Sixty percent of the time we were remotely logging into your computer and fixing it so that we reduced touch labor, we reduced the cost of the account. I mean, just -- it just went on and on. And so that's -- the same thing as what we did in Europe, we're going to do here in the continental United States.

I mean some post, camp and stations that we go to and inventory, you'll find five, six different help desks doing their own thing. And so those are the things that we're going to go after. And we're literally going to go post, camp and station and clean this up because I need those resources to, again, as I said, reinvest to build out this network of

2020 that we want to get to, everything over IP, wireless talk, voice over IP -- I mean, just -- there's so many things that the -- that we need to be doing quickly. And so we need to get those dollars back in and get them reinvested as fast as we can.

MS. MCBRIDE: We'll just keep going. Mary Ann from SIGNAL magazine. Q: My question is about jointness. So this is all very nice, all about the Army, and I'm really enjoying it and all that sort of thing. But I have spent a lot of time covering the - Joint Forces command, which no longer exists. And everybody knows -- (inaudible) -- continue financially or for other reasons only its own service -- (inaudible). So what are you doing in that arena?

GEN. LAWRENCE: Well, would somebody ask a [cyberquestion](#)[cyber question](#), please? (Laughter.)

Q: Actually, cyber is a very good example.

GEN. LAWRENCE: It is very --

Q: I don't mind -- (inaudible) --

GEN. LAWRENCE: So -- well, let me give you one example. I don't -- did you hear Ms. Takai this morning?

Q: I -- (inaudible).

GEN. LAWRENCE: Fabulous DOD CIO. The service CIOs -- we get together every other week, and we roll up our sleeves, and we're going after this because we -- you're right, we cannot afford to continue. I'll give you one example, and then I'll let -- turn it over to Jennifer: something called Unified Gold Master. So there's a change that comes down in our operating system. DISA takes it and puts -- publishes a Unified Gold Master. The Air Force then takes it and kind of puts it in their lab and makes some changes and calls it the Air Force Gold Master. And what does the Army do? We take it and put it in our labs and change it a little bit more, and now we call it the Army Gold Master.

And we said stop the madness. Remember I said we're going to take that CAC card, and I'm going to go to any government computer? We have to baseline it across all the services. And so the service CIO said stop. We're no longer going to do this, and there's going to be -- a policy's going to come out and direct us not to do it anymore. So we're taking things like that on.

GEN. NAPPER: And you probably noticed at the end of her presentation she talked about what we're doing in Europe for a Joint Enterprise Network. If you look at the way we have done business in a place like Europe, which is relatively small, if you don't mind me saying it that way -- compared to CONUS -- OK, there -- we have had an Air Force network, an Army network, the joint network and even in -- a little bit of a Navy network coming into there. And that doesn't make sense anymore, from the transport level or from the way we do the data centers.

And so we are -- this year there's a consolidation of the data centers in Europe, the turning of the network -- the transport piece into one joint environment so that all those are on the same. And then the third piece of that really gets at, then, the (pots of?) citizens and how we work together as a team over there. And so that's the first one we're going after. The second one is in Korea, as you might expect, the joint information environment there. And so we're building from that, then, how to work on the issues here in CONUS.

Q: Thank you.

GEN. HERNANDEZ: So I will take that as a cyber question?

MS. MCBRIDE: Yes.

GEN. HERNANDEZ: Great. I have said from the beginning that the Enterprise services and the Enterprise initiatives are all necessary, but not sufficient. And so the sooner we can get to those, the sooner we can get to the things that are keeping us from being joint now. So we're operating and defending the largest portion of the DOD GIG today because we have to, because it's Army.

When you go to Europe, and you see the synergy there between what EUCOM and AFRICOM are doing, that's powerful. So they're not having service discussions; they're starting to have coalition discussions. And that's really where we need to go. Over time, I believe that this is clearly inherently joint, and will become more and more joint.

MS. MCBRIDE: Defense Systems? We were going to go -- keep going, but Amber (sp), do you want to defer to Barry or --

Q: Can we -- (off mic)?

MS. MCBRIDE: Yes, go ahead. I just saw Barry chomping at the bit --

(Cross talk.)

MS. MCBRIDE: Yeah, yeah. OK, right. (Laughter.) OK.

Q: I was interested in the 15,000 network figure that you mentioned. What are these networks, where are they and -- (inaudible) -- be done with them?

GEN. NAPPER: Right. Well, in the Army, we've identified -- you know, we're going to go back to Ms. Takai -- (inaudible) -- for example, in the Army we have the unclassified network, the classified network, the top secret network, the Corps of Engineers network, the Reserve network, the Guard network, the FORSCOM network -- and I'll just continue to go on. Everybody builds to their own network.

I mean, we've been 10 years at war, and everybody just kind of did their own thing, and we didn't have that governance over it that said "Thou shall not." We now have that, obviously. Sometimes it takes a

crisis to make a transformational change; and in this case, it's called the budget. And so we're going to collapse all of those onto "the" Army Network, as we go through this.

And by doing Enterprise Email first, it was the biggest forcing function, because they will be drawing services off of "the" network, not their own network ~~any more~~anymore. So that's going to force them to go through that.

Q: (So all 15,000 will be collapsed into this particular Army network ?)?

GEN. NAPPER: No, that -- she -- what she was talking is the DOD --

GEN. LYNN: No, the DOD network --

GEN. LAWRENCE: It was the DOD network, the department --

GEN. NAPPER: -- because all those other agencies --

GEN. LYNN: Or smaller stuff -- (inaudible) --

GEN. NAPPER: -- Army, Navy, Air Force --

GEN. LAWRENCE: Right, right --

GEN. NAPPER: We have all those 22 agencies out there, too, yes.

MS. MCBRIDE: Andrew White with Digital Battlespace.

Q: (Off mic) -- what do you make of Vincent Viola's -- (inaudible) -- yesterday about ~~cyberwarfare~~cyber warfare?

GEN. HERNANDEZ: I liked it. Actually, I liked what he was discussing on how to go after the human capital piece of that. So I was actually taking him up on his offer where he said, oh, I'll share with you how it is we ferret out who are our cyber experts. So I'm hoping he'll send me that so we can use that.

But the human capital piece of this is becoming more and more important because, as you know, science and technology, those folks that really want to do that are declining in the United States. So finding those people that have those skills and really love that business, we want to get after that. So we are working a human capital strategy, and I think this will just be another arrow in that quiver. So, absolutely, we're going to take him up on that.

MS. MCBRIDE: All right, J.D., from Army News Service.

Q: Yes, Major General Lynn, when is this soldier avatar? I think that's pretty cool. I'm getting psyched up. When do you foresee (seeing them ?)?

GEN. LYNN: They're already doing tests on it with the Maneuver Center of Excellence; also the aviation, and also Mission Command down in CAC at Fort Leavenworth. They've already built some avatars. They already have built some gaming systems. They've already laid out some of the maps -- the digital maps, for the actual areas that we've used in Afghanistan, for example. So it's really very -- it's new; it's just now taking off. But the quality is really, really pretty good. They've got a neat game engine, and they've got a team that's working that. And so now we're bringing all the centers of excellence in to put a full spin on what it means to do a war fight. So it's pretty exciting.

GEN. NAPPER: Recruitment Command has a --

Q: (Off mic.)

GEN. NAPPER: Recruitment Command has one version of the game already out.

I brought it home and my daughter and I played with it a little bit. Actually, she taught me how to build an avatar. (Laughter.) And you do have to put in, you know, your height and weight, your gender, your PT score, your marksmanship, and then you go through basic training; you then can get qualifications in the game itself. And so it's kind of giving the soldiers a feel for what basic training will be like. And then there actually is initial advanced skills training in -- (inaudible). And it's kind of fun. It's available at most -- (inaudible). The second version is out, which is much better quality on the avatar and the game itself. So it's worth playing if you want to try it.

GEN. LYNN: And they really look -- when they assess something, when they come in, just like you can get an ID card, you get an avatar and it's going to look like you. (Laughter.)

Q: (Inaudible) -- talking about -- (inaudible)? This will be available in months or years or what time frame?

GEN. LYNN: They're working it right now. So --

GEN./MS. : I think months.

GEN. LYNN: So probably months.

MS. MCBRIDE: OK. What we're going to do now --

(Cross talk.)

Q: I wanted to ask General Lawrence if you could get into -- (inaudible) -- where's the noise coming from, what's holding you back?

GEN. LAWRENCE: Right, right. Yeah, the -- when I commanded NETCOM, I used the analogy a lot -- (inaudible) -- is you can only have one quarterback and one playbook on the field. If you're trying to -- if you're trying to score, if you've got six quarterbacks or six playbooks

running all over the field, your chance of scoring is really reduced. And so the key is to have that one quarterback and that one playbook as we're going through it.

So the first thing we did is we have the network authorities, which we called the DAAs (ph) out there that had the authority to say what was going on the network and configuring the network. So we had a lot of people who thought they were in charge of the network. So as we were trying to put in a private email out there and we couldn't get one post to talk to another post or one individual to talk to another individual, we brought in a team and said, what's going on here? Well, we found fire walls where there weren't supposed to be fire walls. We found people who bought an application or a service, they put it on there and it wasn't compatible with another one. And so -- and we're just finding all kinds of things on there that should not be on there.

And so now what we're doing is, we're putting out, you know, the directive cease and desist. No one can touch the network. It has to come to a single individual that has the architecture -- and this is the other piece; this is really big -- is as we build out the architecture from end to end -- we've never really done that. We've kind of done the post one and then there was this tactical network out here, and never should the two talk to each other. Well, we can't win if we don't have -- if you're not sitting at Fort Bragg being able to talk to Afghanistan, and that's the network that we're going to be building the architecture.

But that's also going to include in the future the logistics piece, the medical piece, the intel piece, and so that it's all siding with the same standards, the same configurations. No matter where you're fighting in the world, when you connect anywhere, it -- you'll -- it will look the same, it will act the same and you'll be able to touch it.

I remember when I was the J6 of CENTCOM, I went into the VIP lounge because my aircraft broke down and we were trying to get it fixed. As I go into the VIP lounge to log on -- and they won't let me log on to the network -- so I called up the comm squadron -- (inaudible) -- the Air Force, comm squadron commander. I said, come see me. And so I sat there and I said: Why won't you let me log on?

And he says, well, this is an Air Force network, and we have higher standards than the Army.

And I go, well, I'm the J6 for the entire theater, and I think I should be able to log on! (Laughter.) So that's the kind of things that we're working through.

Q: Do you have a time frame for where the network is back at zero, where you want it to be?

GEN. LAWRENCE: Well, unfortunately, I am convinced that if I -- if we could just stop the war and start from scratch, we could do it faster and cheaper. But unfortunately we don't have that luxury, and so we're having to do it as we go. But we've had some huge wins, General Huggins, down at Bragg.

(Cross talk.) GEN. NAPPER: So I -- while General Lawrence is working very hard on the governance and on the architecture so that we know what to build to, at the same time, as we -- we're kind of using the first implementation of an enterprise capability, which happens via email, to help us find where we have problems in the network. And so as each post and camp and station goes over to the Enterprise Email, just before we migrate them, we go in and we look at those networks and make sure they have actually checked all the configurations and put them back to (so that you would call it ?) the baseline or ground theater or whatever you want to call that -- (inaudible). OK.

So we're doing that at the operational arm as we go forward with each post implementing it its email, and that is a huge difference.

The second part is that active directory domain collapse I was talking about -- that takes those from having many different areas where we segregate out information into one shared information space. So now there's no reason to have all those extra firewalls or impediments to communication, and now we'll be able to scan all the way down.

So it helps our business of the operate, (defend ?) on a daily basis; at the same time, executing where we need to go for one network on the long-term vision.

MS. MCBRIDE: OK. So at this point, I'm going to open it -- I'm going to bring in the bloggers and media who are on the call. And I'm going to go down a list here. It's not going to have a whole lot of logic, but I think this will expedite, since we have about 15 more minutes, and then we'll be cutting off.

So can -- let's test and see if you're still there. Is Army Times there?

Q: Yeah, this is Joe Gould. I'm here.

MS. MCBRIDE: OK. So why don't we start with you?

Q: OK. Thanks. General Lynn alluded to the use of commercial off-the-shelf technology, and I was curious what the other panelists think is the future of smartphones in the Army. Is the network at present really equipped to, you know, handle some kind of mass deployment of smartphones? And how does it all kind of fit together with the existing radio technology that the -- that the Army's really working right now?

GEN. LAWRENCE: I'll take that very quickly and pass it to my teammates. This is Susan Lawrence.

The key -- you brought up a very good point, and it's the key of balancing -- being able to have access to the information -- the freedom and flow of information, and then protecting the information. So there's no doubt we're going to have millions of billions of (sensors ?) here in the near future on this network. We're going to have mobile devices on

the network. And so the key is, how do we bring them on to -- and I talked a little bit about it on the other end. So at the back end, we have a computing environment that's going to meet a common operating environment standard and configuration. We're going to direct what that is.

Then on the front end, what the soldier has is a device. As long as you can meet the security requirements -- so if you are discussing for official use only, if it is government-sensitive information, your ability to sign and encrypt and validate that that is you is what the requirement is going to be for that mobile device. And those are the things -- and then Mr. (inaudible name) is going to come out with some further policies on how we're going to do this as well.

But that's the key -- balancing flow of information to protecting the information as we work through this in the mobile device environment.

Q: And are we close to -- you know, we are close to cracking that, that question?

GEN. LAWRENCE: Well, we are, and I'm working with big companies, you know, partners -- Apple, Google, different companies -- to say that's what our requirement is going to be.

And we're testing one device right now that in fact you can embed -- it's an iPad-like device that you embed your CAC card in and actually now we're -- have the ability log on to the network and sign. And so as long as industry can bring those to the table, those are the devices that we want, that we're going to seek out.

And so we're working with a lot of partners on this, but we're really excited about this, and I hope we'll have a decision within this week that that device in fact does work, we can sign and encrypt. And if that's the case, then we're going to put on the shelves very quickly for our units to be able to procure.

OK.

GEN. HERNANDEZ: Joe, this is General Hernandez. Clearly, from an operation standpoint, I can't wait to get them out there. It wasn't too many months ago that I was on the end of how come we can't have this. (Laughter.) Now from vulnerability standpoint, I'm at the end saying let's make sure that we continue to bring them on at the rate that allows us to ensure that we maintain a trusted and secure environment.

We are engaged with the team here in all the NIE work. And we have a team that is part of those evaluations that are really looking at what vulnerabilities might these bring to the network and how can we reduce those vulnerabilities so that they can be trusted and secure, so that we can get them into the fight as soon as possible. And I think that's a key piece of what we're gaining from our NIE work.

MS. MCBRIDE: I think that has answered our question. Let me move on to the next. I know we have -- I thought I heard Federal News Service. Is that correct? (No audible response.) OK, let's move on to Inside the Army. Sebastian?

Q: Yes, thank you very much. I have a very quick clarification from General Lawrence, please. You used the phrase "a smaller but much more capable Army." I'm wondering if you can give some context for this. And then my question is, what is the Army doing to help protect the supply lines for important weapons programs?

GEN. LAWRENCE: I'll ask for a clarification on that second one.

But the first one is, we're getting directions from the department -- Defense Department to take a look at drawing down our forces. And so we know -- remember the surge we did going into Afghanistan. But we will be drawing down those 25,000 additional soldiers that we have brought in--in the next couple of years. We also anticipate, based on the reduced budget, depending on how reduced the budget is -- then we're probably talking taking forces out of the inventory. And those are efforts that we're looking at right now. Nothing definitive on it, but that's just the reality of -- depending on how much -- how small the budget's going to be or what the cut from the budget's going to be will determine if forces need to be taken out of the inventory. And so that's what we're -- you know, I think we can say with pretty high confidence that there'll be forces taken out of the inventory. We just don't know how many at this time.

Q: Mm-hmm, OK.

GEN. LAWRENCE: So I think I'll reword the second question and make sure it's the right one. I think you meant protect the supply chains for the embedded processors of our weapons systems is what --

Q: Yeah, the Defense Department has this program, Supply Chain Risk Management.

GEN. LAWRENCE: OK.

Q: I understand the Army has a piece in this. So I'm trying to get some insight on what you've learned, what steps are being put in place and so forth.

GEN. LAWRENCE: Yeah, the key on that is as we acquire technology and capabilities, a lot of the time our big companies partner with international companies. And so that's called supply chain management. When we are taking a look at procuring something from a company, who are your partners? And so we do that before we issue a Certificate of Networkiness to allow something onto the network.

So for example, if your partner's Iran, we may take a second look at it. If your partner's the U.K., then it's probably OK. And you know, those are the kind of things that we're now looking at because so many of the -- of the international companies' technologies are very

advanced, and so they're finding that marriage there between the -- our national companies with our international companies. So that's the supply chain management that we get -- that we get -- we take a hard look at.

Q: Any results so far? Any decisions made on how to alter processes or so?

GEN. LAWRENCE: No, I think the process we have in place is a good one as we do the background investigation. And then when we bring them on and test them is where we find out where the vulnerabilities are or are not, and especially their interoperability capabilities as we work through it is where -- what -- (inaudible).

GEN./MS. : And the quality control.

GEN. LAWRENCE: And the quality control of the product.

Q: OK, thanks.

MS. MCBRIDE: OK, North Shore Journal.

Q: Good morning, folks. Chuck Simmins from America's North Shore Journal. I wanted to ask a cyberwar question. With the apparent success of a cyberattack on the Iranian nuclear enrichment program and a bunch of stories for the last week about hacking things like insulin pumps and cardiac pacemakers, what is being done to ensure the security of the nondesktop computer -- computerized parts that the military uses?

GEN. HERNANDEZ: I think what you're seeing is what we're all seeing, is that the threat continues to evolve. We have gone -- clearly we know we're into the exploitation, and we see attempts to penetrate us every day for the purpose of exploitation. We see attempts every day to -- in the cybercrime arena to get individuals' personal identifiable information that might be beneficial to them. But we're also now seeing an increased capability to do those things that clearly can be disruptive and the potential for what you're talking about, increased capabilities on higher-end threats that might have the ability to destroy things.

A key component to that is really our ability to protect critical infrastructure. Critical infrastructure protection is a responsibility of department of homeland defense, but at the same time, Department of Defense and each service has a clear requirement to ensure that we're doing the things necessary to protect our critical infrastructure.

We're working hard with the Headquarters Department of the Army, specifically inside of force protection, to lay out what types of capabilities provide the most significant vulnerabilities that we need to be sure that we're protected against. And that work is ongoing. And I've said I don't take a lot of comfort in being a service that might be good at this, because as a nation we're probably only as good as whatever our weakest link is with respect to critical infrastructure.

MS. MCBRIDE: We have time for about one or two more questions. Government Executive, Bob Brewin?

Q: General Lawrence, can you update us on satisfaction with Enterprise Email? I've had comments plus I've talked to folks who are real unhappy with the switch. And I know you had a stand-down and have started up again. Why were folks unhappy? And what are you doing to make them happy?

Thank you.

GEN. LAWRENCE: Bob, what a great question. Thank you.  
(Laughter.)

Well, first of all, let me tell you the goodness of it. First, it is not just the economics of being able to deliver this capability much cheaper in a managed services capability, but more importantly, to reach our joint partners. You know, today the individuals that are -- successfully now, by the way, we've transitioned over 90,000 individuals now. I've been on it since March.

And now I have -- some of the pluses -- I have an unlimited mailbox. You know, how many of us, you know, you get that notice that says you can't use your email anymore until you delete some of your old emails. We have unlimited access now.

The other thing is, I can actually look across the Department of Defense and get somebody's email addresses on a global access list. I mean, is that not, you know, just a fantastic thing? You know, before with all these disparate networks, if I wanted to reach a doctor in the medical community, I couldn't even see him. Well, now I can see everybody, which is a good thing and a bad thing, in that do you know how many -- I have a Major General Steve Smith that works for me. Do you know how many Steve Smiths there are in the Department of Defense?  
(Laughs.) And so we're working through those kind of things.

So the pluses are just, you know, overwhelming on the services. And like I said, I can go anywhere with my CAC card now. And I'm going to let -- Jennifer's done more traveling and she can explain to you that experience as we go through it.

The bad experience was the incompatibility of software. Latency. It was those things we had to do. And this is why we stopped and did a strategic pause, because we want the user experience to be a positive experience. And so we said, OK, stop; there's no reason for us to continue; let's take this pause; let's go clean up the network; let's get those standards set out there. And now we're getting ready to start up again. Right, Jennifer?

GEN. NAPPER: Yes, ma'am. So, Bob, in kind of like full disclosure here, we knew we had challenges on the network in CONUS because of how many people were running pieces and parts, and an inability to look at the entire network top to bottom. We also thought we knew what kind of configuration (would be required ?), the desktop and

the network, in order to do this Enterprise Email. We were not correct on the complete configurations.

So there were some settings that some of the early adopters, like General Lawrence and General Hernandez and I, had a little bit more what we saw as latency, which means it took time for the software on the computer to reach all the way across the enterprise and talk to the server at DISA. OK. And that (software -- because we ?) also changed the identity management. So that gave a little bit of a challenge there.

When we went back and re-looked at those configurations with our engineers, we now have a very good -- I would call it a 90-percent solution of how the network and those end devices have to be configured in order for us to be able to draw services from the enterprise. And so now we have a premigration checklist, if you will, like we do in just about everything else in the Army, pre-execution checklist.

And we make folks follow that precisely. They don't get a vote.

And when we know that they are reconfigured, then we do the migration, and they don't even know that they've been migrated. The only way they would know is they're required to log in a little differently now because you're reaching the enterprise.

Since we stopped the pause, restarted -- stopped the pause and restarted migrating, we did two test locations, Fort Lee and Fort Leavenworth. And we have had absolutely no issues at those two locations. It took about -- less than a minute per email account to migrate now. It's way down. We started off -- some of us in the beginning were 10 or 15 minutes. That's a sign that you have a problem on your network. And the folks the next morning came to work and email was up.

So we knew that it was going to be painful in the beginning. We did warn folks. They didn't really want to hear it, but we did warn them. And I think that we now have a much better process and configuration control going forward.

And so we'll start up again right after Labor Day with a little more intensive migration.

MS. MCBRIDE: We've reached the end of the hour. And I apologize that not everyone has had a chance to ask answer (sic) questions. You can follow up with my office or with General Hernandez's office, his public affairs officer r.r., and I will -- well, I can give you right now my email: margaret.m.mcbride2.civ@mail.mil; and patricia.e.ryan@us.army.mil.

So again, I thank all the generals who were able to participate today. This is really great that -- any further -- any ending comment?

GEN. HERNANDEZ: Yeah. General Hernandez. I'd like to make just one final comment here.

A lot of discussion on enterprise initiatives and enterprise services, and I applaud them all. And I keep saying the faster we can get to them, the better we are. And I am comfortable with all the efficiencies that we will gain that others are counting on.

I am really more excited about the effectiveness that this will bring to our ability to defend our networks and the ability to see ourselves, to see the threat, to see the cyber terrain and now really start getting into more of an active defense and the types of defense strategies that the Department of Defense has asked us to look at in their cyber security strategy.

GEN. LAWRENCE: Thank you. And I'm so excited about the time we're entering. I call this the year of action. So we're going to move very quickly. I think you'll see in the next 18 to 24 months a very different network, a very different environment, one that we can secure more easily and have trust in. And that's our -- that's our personal goal. But our partnership with our service component commands to cyber-operations is absolutely critical because that's -- that's why we do what we do. And I'm excited about it. It's a neat time to be in this business.

END.