

Department of Defense Bloggers Roundtable With Giorgio Bertoli, Senior Engineer, Information and Network Operations Division; Communications-Electronics Research, Development, and Engineering Center (CERDEC); and Stephen Lucas, Chief Engineer, Cyber Security and Information Assurance Division, Space and Terrestrial Communications Directorate, CERDEC
Subject: The Cyberspace Technology Landscape Time: 10:00 a.m. EDT Date: Thursday, August 25, 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 for more information.)

LIEUTENANT TIFFANY WALKER (Office of the Secretary of Defense Public Affairs): Good morning, everyone. I'd like to welcome you, including Giorgio Bertoli, Stephen Lucas and our bloggers, to the Department of Defense's Bloggers Roundtable for Thursday, August 25th, 2011. The time is now 10:00, and we'll begin our program.

My name is Lieutenant Tiffany Walker, with the Office of the Secretary of Defense Public Affairs, and I will be moderating our call today. Today, we are honored to have as our guests Giorgio Bertoli, senior engineer for the Information and Network Operations Division, and Stephen Lucas, chief engineer for the Cyber Security and Information Assurance Division.

We are honored to have you as guests today, gentlemen.

Before we begin, a note to our bloggers on the line today: Please respect our guests' time by keeping your questions succinct and to the point.

We will begin with statements from our guests, followed by one question per blogger in order of appearance on the call. Please wait for your name or blog to be called. And if time allows, we will continue with questions after the first round.

And finally, please place your phone on mute but not on hold if you're asking your question. This helps ensure a clean audio recording for transcription and your use later.

Can I ask who -- what blogger just joined the line today?

(No audible response.)

LT. WALKER: No? OK. We have --

Q: Petty Officer William Selby.

LT. WALKER: OK, thanks, Mr. Selby. We have three bloggers on the line today: Tom Goering, Zach Rause -- Rausnitz -- sorry Zach -- and Dale Kissinger.

We will begin with an opening statement from Mr. Bertoli and Mr. Lucas. Go ahead, gentlemen.

GIORGIO BERTOLI: Good morning. My name is Giorgio Bertoli. As mentioned, I'm the senior engineer for the Information and Network Operations Division. Primarily, the technologies that I have been focusing on for the past 10 to 15 years have been revolving cyber -- before it was actually even called cyber -- primarily on the offensive side of the house, in terms of electronic warfare and computer network operation technologies.

STEPHEN LUCAS: OK. My name's Steve Lucas, and I'm the chief engineer for the Cyber Security and Information Assurance group within what's called the Space and Terrestrial Communications Directorate out of CERDEC. I've been in the -- I guess I've been in the business for a good 25 years now; initially in -- my main focus was in cryptography, key management, the information assurance domain. I'd say probably within the last 15 years or a little more, I've been dedicated to the computer network defense portion of the cyber, looking at interest in detection systems, firewall technologies, things like that. LT. WALKER: All right. Well, thank you both. I appreciate it, Mr. Bertoli and Mr. Lucas.

Now we'll take blogger questions. Tom, go ahead. You're first.

Q: Oh, thank you. My name's Tom Goering with, ironically enough, Navy CyberSpace, navycs.com -- although I do nothing with IT. My question does come to -- each service has set up its own cybercommand, creating stovepipes, if you will, by -- through -- with each service. Does -- is that going to create, or has it created already, problems with hardware compatibility, network compatibility across services? So, and you could take it from there. I think you know where my question might be going. Is -- are we having some issues because of the different commands and the ways that each service has determined to set up their own (networks ?)? Thank you.

MR. BERTOLI: I'll give it a shot. Well, first of all, let me caveat by saying we're more on the science and technology research and development side of the house. So when you're talking operational, we're probably not the most familiar with that.

That said, it's a perfectly valid question, but I would say that it's probably even too early to tell at this time whether those issues have arisen. Army Cyber, as a matter of fact, has only been active for less than a year now. They're still trying to stand up and come to full

strength. On top of that, you do have the overarching umbrella of Cyber Command that is supposed to prevent those specific stovepipes from happening. How successful the whole thing will be? I honestly believe that that's yet still to be determined.

LT. WALKER: OK, thank you, Tom.

Dale, follow-up?

Q: Not right now, thank you.

LT. WALKER: OK. Zach, your turn.

Q: Hi, there. I'm wondering about (consumer ?) gadgets in the workplace, and sort of the issues, like, surrounding, you know, cybersecurity and network security, and whether government agencies are moving too quickly or too slowly with this, just in general.

Q: Are you folks sitting more on, like, the defensive side of the house?

Q: Yeah.

LT. WALKER: Zach, could you please repeat that question, and a little bit louder? It was hard for us to hear you on this side.

Q: Oh, sure. The question is just about consumer IT in the workplace, and specifically within the defense and cyberdefense workplace, whether the integration is moving too quickly, too slowly. Was that loud enough?

MR. LUCAS: OK. Again, I guess when it come to us trying to leverage commercial off-the-shelf types of technologies, a lot of issues stem from, you know, where you have to place it within the -- say, the Army's architecture, if it has to tie to what we call our (secret high ?) networks. We do a lot more rigorous, say, analysis of what security feature sets or security protections these types of devices include, and a lot of times they don't have the right levels of protection mechanisms incorporated into them.

So at least from an S&T perspective, we try to develop technologies -- security technologies that can easily integrate seamlessly into those devices. But for the most part, the leveraging of the commercial technologies is a rather slow process.

Q: Great. Thanks.

LT. WALKER: All right, Zach, thank you.

Dale, you're up next.

Q: Good morning. This is Dale Kissinger from MilitaryAvenue.com. My question concerns the LanWarNet conference. Can

you explain a little bit about the conference? Is it a joint conference? Is it the first one? Just give us some details on that.

MR. BERTOLI: Yeah, I mean, that will probably be a better question for the sponsors of the conference, which is FC -- the Army -- what does it stand for? I don't even know.

MR. LUCAS (?): Armed Forces Communications Electronics. MR. BERTOLI: It's Army (sic) Forces Communications Electronic Association. So this has actually been a recurring conference that happens annually, but I must admit I don't know when it actually started. But every year right around this time in the same venue, they have this conference. And it's really just one of many conferences that DOD has to bring professionals together within the world of communication electronics, and this year cyber was the theme to discuss some of the issues ongoing.

Q: OK. And what was your role? Did you speak at the conference or were you questions and answers, or just participating in the conference?

MR. BERTOLI: No, we actually had a briefing, a panel session. It was actually yesterday. We had a brief that we presented to the conference.

Q: And can you tell us what that panel session was about?

MR. BERTOLI: Yes. Well, we spoke about the future of cyberspace technologies from an S&T perspective. In included kind of like a small, futuristic look at what the environment is going to look like in the next two to three years. And then I focused more on some of the challenges in offensive technologies, electronic attack, electronic warfare, while Steve is more of a computer network defense guy, so he was focusing more on the work that he's doing in CND. I believe the slides will be made available for the -- for all the briefers, on the website after the fact.

Q: OK. Thank you very much.

LT. WALKER: All right, Dale.

We're going to have Mr. Selby ask a question next. He's writing the story for the DoDLive blog. Go ahead, Mr. Selby.

Q: Mr. Bertoli, you just said -- you kind of discussed that you were talking about what Cyber Command will look like in the next few years. Can you comment on that and give us a little bit of an overarching view of what it will look like in the next few years?

MR. BERTOLI: Well, I apologize if I -- if you misunderstood me. I said what cyberspace would look like, not what Cyber Command would look like. I have no idea what Cyber Command's going to look like in the next few years.

However, cyberspace, one of the three -- it's really -- we have three key tenets, if you will, that we're kind of preaching that kind of drive our S&T investment. And one is pretty much that everything at the user level is going wireless. So the last link, whether it to be to your house or to you as a person, is obviously wireless.

As a matter of fact, it's wireless now. There's very few wires that we have left.

And two, everything is becoming an IP service as opposed to a dedicated communication link, right? So an example of that would be your FIOS TV or your cable company's TV, right? So I want to buy TV; that's the service I want to buy. Why is it that I have to watch it at my house? That's something a user wants to get away from, right? If I happen to be on the road and I have my phone or my iPad or whatever that might be, I want to be able to watch TV, which I bought and paid for, wherever I happen to be, not just at the house. So that's a huge paradigm shift that's happening.

And last but not least, the last tenet was kind of related to that and the fact that the physical connectivity to that service should be completely irrelevant to you as a user, right? It doesn't matter whether it's wireless, wired, fiber-optic; shouldn't matter, right? Whatever (sic) I happen to be, whatever the best connectivity option for me at that level, that should be available to me, (transparently ?).

Q: Thank you, sir. What are some of the newest projects you're working on for -- with cybersecurity -- or cyberspace? I'm sorry.

MR. BERTOLI: For cyberspace?

Q: Yeah.

MR. BERTOLI: I guess we'll both answer this one.

Now from the offensive side, I'm going to stay very high-level just because of classification issues. But one of the biggest things we're working on right now is a concept of frameworks, having a common core baseline, so that we don't keep reinventing the wheel all the time whenever we build different tools and technologies.

It's a big problem right now, specifically just because we happen to have been in -- you know, in a very reactive war-fighting mode for a long time now. So we tend to build point solutions that need to -- rapidly deployed, but that costs you in the long term because now you have a bunch of solutions that don't really interoperate with each other, and you're burdening the user with having to learn different tools as they come out very, very rapidly. So we're really more on the architecture concepts, framework concepts that allow you to plug in new capabilities without changing dramatically, say, the look and feel of the technology, so that the training is much reduced; and also, from a development point of view, that we can develop faster, because we have a common code base to work from.

Steve, do you want to add to that?

MR. LUCAS: Yeah, from the -- from a defensive perspective, regarding the frameworks that Giorgio was talking about, a lot of the present protect -- or defensive tools that are -- that are currently deployed on our networks, whether they'd be intrusion detection systems, firewalls, intrusion prevention systems, like Giorgio mentioned, they've stovepiped. They don't interoperate or communicate amongst each other. So it's very hard to correlate alert information, you know, acknowledgement of potential threats against our networks, across these various devices.

So as part of this framework, we want to provide that sharing of information between these devices, so that we can better our overall defensive posture for the network.

Other areas from the defensive perspective that we're looking at is, when it comes to our defensive posture, traditionally we've always been in a reactive type of mode. So basically you detect the threat and then you try to respond to it, OK?

From an R&D perspective, we're trying to get out in front now and make our protection types of mechanisms more proactive, where they sort of can now try to predict what the next move of our adversary will be, OK, and either provide some sort of intelligent reasoning on where we think, you know, the adversary is or what particular network component or service he's going to go after, or even possibly, down the road, make our network look something that it isn't to the adversary, to make his job a lot harder, OK?

For instance, if he tries to find a critical service or application, OK, we make it eventually look like something that it's not, OK? He's trying to find an email server. We'll make it look like a Web server, OK? So these are -- these are types of technologies that we're looking at.

LT. WALKER: All right. Oh, sorry. Thank you, sir. We're going to go ahead back around to Tom Goering.

STAFF: So we have Jared from Federal News Radio. I didn't know if -- Jared, did you have a question?

Q: I'd love to, if I might.

LT. WALKER: Go ahead, Jared.

Q: This concept of everything over IP has been sort of a theme down here at the conference. Can you guys talk a little bit more about the ways in which that may be increases the attack service to the -- for the entire -- I guess to the entire Defense Department? And what sorts of services do we now have to think about as potential threat vectors that we never had to worry about in cyberspace before?

MR. LUCAS: Well, I think it has -- I think it has a lot to do with the ubiquitous, you know, access. Basically, you're looking for access for just about anywhere within the network. So you want -- you know, when you want access to a particular service, OK, I can do it.

And I guess, basically, looking at it from an Army tactical network perspective, OK, you've got to think about it maybe with respect to the need to do, OK, one minute I might have access to our traditional RF Army tactical networks, OK? But say for instance, now with this push now to do more cellular type of communications -- you know, rely on the smartphones, the iPads, those types of communication devices -- there may be an eventual need to leverage a commercial infrastructure, OK?

So say the -- you have a roaming user out there on the battlefield, OK? He might have a -- you know, at one minute he'll be able to access our military mobile network, OK? Let's say he roams off and now he comes into roaming distance of commercial infrastructure, OK? So we want to do, like, a seamless auto hand-over to allow him to roam out on that commercial infrastructure.

Now there's a lot of implication securitywise with him doing that, because a lot of these commercial infrastructures don't have a lot of what we call the authentication-type of techniques, OK, to authenticate him to that network, OK, to protect that information that he's now going to send across that commercial network, things like that. (Do you ?) want to add to that?

MR. BERTOLI: Yeah. Well, yeah, it's really a paradigm shift. I'm going to -- I'm going to speak a little computer network (defend ?) here, as opposed to offense. But the way -- the way historically -- and this is not just DOD -- the way historically everybody's been designing CNDs (ph) -- really, you know, you have a gateway -- a strong gateway defense perimeter, right? The firewall's messed up. And then even -- because that wasn't enough -- you had strong host-based intrusion detection and anti-virus protection.

Well, the whole concept of IP as a service, especially when it comes to things like cloud computing, right, that destroys that paradigm, because now all your computing and all your processing is done out there somewhere. And your border and your host protection are no longer -- no longer relevant. All the protection has to now reside out there in the cloud with the (applications ?) that happen.

And then you're assuming, then, that your coms channel from where you happen to be to that service is now trusted, right? So it's really just a completely different way of thinking about security in terms of what we used to be able to do to this new construct. And that's yet to be -- you know, we're just scratching the surface on how -- the implications of that -- (inaudible).

Q: I guess, more to the point, I'm talking about -- I'm looking for things that are now delivered over IP that previously weren't, that used to be in the analog domain.

MR. BERTOLI: Oh!

Q: Attackers come at you through your toaster or something --

MR. : Oh, OK. (Laughter.)

MR. LUCAS: One thing -- on thing of particular interest is voice. Right now, voice is digitized, OK? It's sent over what we call voice over IP. With respect to authenticating that voice, before it was easy. You know, it was analog, OK? Somebody could reasonably differentiate that -- I -- that sounds who I think it is. Now you're digitizing that voice, OK? It may be a lot harder now to assure authentication of that individual, OK?

MR. BERTOLI: Yeah, I mean, from an -- from the -- from the DOD, I think, IP from the -- its first conception really took hold, we don't -- there's not a lot of proprietary waveforms anymore. I mean, even the radios, while they -- they're physical channel is still military-grade, the higher levels do have IP addresses. So everything is IP.

Now, I actually think that one of the more interesting things would be if we ever do get to IPv6, and you do follow that model. That makes it actually even more interesting from an offensive point of view, right? Because now if everything truly does have a routable IP address, now you truly expose your entire attack surface, right? So there's something to be said about network address translation and net protocols in terms of security benefits that are provided.

Q: Thanks.

LT. WALKER: All right, thank you, Jared.

Tom, do you have anything else?

Q: Well, actually, it was leading into my next question. The VP -- IPv6, excuse me, the technologies come with that, the -- I believe there's actually going to be, or there is built-in security -- at least somewhat. But how are we going to leverage that in our -- I thought we were actually already starting to use some of that (sic) technologies? Thank you.

MR. BERTOLI: No, I don't -- I mean, a long time ago, there was a memo -- (chuckles) -- that came out that said that all DOD systems are going to be using IPv6 by some -- what was it? By 2002 or something? (Laughter.)

Q: It's been a -- it's been a while.

MR. BERTOLI: Yeah, it's been a long time.

Q: It's been a while.

MR. BERTOLI: So obviously, that hasn't happened. And the reason why it hasn't happened is because the transition is very, very

difficult. As far as I know, we are not using IPv6 yet. Now, that said, everything is IPv6-compatible.

Q: Right.

MR. BERTOLI: So I think there is -- there is some time in the future that they hope that, when they reach enough center of mass, they can flip the switch and everybody transitions over to IPv6. But that is not on the horizon yet.

So IPv6 is definitely a -- you know, supposedly, a better protocol and definitely can provide a lot more capabilities, including security. But with that security comes additional overhead, additional bandwidth issues. So especially when you start pushing things to the tactical edge, those things have huge implications. So that's why it's been slow in happening.

Q: Roger that. Thank you.

LT. WALKER: OK, thank you.

Zach?

Q: Hi. Yeah, I'm wondering if you think there are any issues that aren't getting the attention they deserve or that we'll be seeing become more prominent in the next few years?

MR. BERTOLI: Ah, that's a good one. You stumped us.

Q: (Chuckles.)

MR. BERTOLI: Give me a second. (Pause.) Well, we actually -- I'm -- I got to be careful here, right? But we're actually part of an OSD-level -- Steve and I are both part of an OSD-level science and technology steering committee that's trying to figure exactly that out. It's a cross-duty organization that includes all the service labs and some of the other DOD organizations, to lay out a road map of what investments should be made in the next several years.

And several topics came up. I guess one of the big ones that I think I can talk about further safely is in terms of metrics, right? So how do you measure -- how do you -- how do you put some math in the world of cyber, right? So, for example, if I wanted to ask a question of: Hey, if I add this security device, this firewall, to my network, well, can I quantify how more secure really am I, right? What -- you know, was I a four before and am I a five now? Is that really better?

There's really no way of doing that right now. There's no math that says: How trusted are you versus somebody else, or how secure is this network versus that network? All you really have is a gut feel and a kind of a common, best-practice approach to doing things, but there's no really math or theory behind computer network defense -- or offense, for that matter.

Q: Right.

MR. BERTOLI: So I think that's a huge need that people are really looking at now.

MR. LUCAS: Yeah, because when you -- when you evaluate a cryptographic type of device for its -- for its strength in -- of its security, you do a lot of what we call formal proof, OK? And this is the scientific or mathematical rigor applied to analysis to ensure that you can't bypass, OK, the cryptographic portion of -- you know, of -- for the encryption and decryption piece. So, like Giorgio's saying, we're trying to see if we can leverage that type of a science into, you know, determining how much better are we making our security posture on our networks by developing these certain technologies.

LT. WALKER: OK, thank you both, gentlemen.

Dale?

Q: Yeah, my question concerns social media. Has the Army's acceptance of social media, such as Facebook, Twitter, et cetera there, complicated or made your jobs more difficult?

MR. BERTOLI: Yes.

MR. LUCAS: Yes. (Laughter.)

MR. BERTOLI: I -- I'm going to be careful on this one. I mean, obviously there are benefits to providing services like email and social networking to our war fighters, in terms of morale. I was actually deployed in the first Gulf War, and I wish I had those capabilities at that time; I didn't. So I can understand it. However, you definitely have to take into account the implications that it has.

However, I would say that most of the issues are probably more prevalent on the -- on the operational security side of the house than they are on the information security side of the house. I would -- I'm probably less worried about that whatever -- the -- because the machine that they use is stand-alone computer that has these services that they share. So even if that one machine is compromised, it doesn't reveal anything drastic.

However, I think the biggest challenge is making sure that everybody's trained to not reveal certain information that you wouldn't want to have the general public know about current operations.

Q: So it doesn't really affect the ability to protect the 'net, but it does cause problems for OPSEC. Is that -- does that mean we have the lead on issues for civilians, commercial side, too? Do you think that the military is helping develop the kind of protection that we have for the civilians, or are they leading us?

MR. BERTOLI: Yeah, I don't know. I mean, they're kind of different problem sets, I mean, depending on where you look. At the GIG

level, right, at the bases and stuff, pretty much the Army just looks like a giant corporation. The challenges are very, very similar, and we rely on COTS product, just like everybody else. So I would say that industry, in that regard, is probably the driving factor, that we leverage their technologies. Q: Right. Right.

MR. BERTOLI: Now when you push the tactical edge, which is where Steve specializes --

Q: Right.

MR. BERTOLI: -- then I think it's just the opposite.

MR. LUCAS: That's where you -- you know, when you start getting down into our RF-based or our radio-based networks, OK, this is where -- this is where we -- we're a lot different from the sustaining base or the strategic side of the house, where they rely on, you know, big pipes for their -- for their communications links, things, like that, OK?

Our environment at the tactical edge can be, you know, very resource-constrained, OK, within our -- within our platforms, OK? Our com links are very low bandwidth, for the most part, the further you get down, OK -- say battalion and below, OK? There's a lot of disconnection or loss of those links in those types of environments. So you don't have the reachback capabilities.

So a lot of the security services actually are pushed further down toward the tactical edge, OK, because of the disconnected type of environment, because you don't have a lot of those reachback capabilities.

So there's a lot of more unique types of -- at least in our case -- Army-specific capability that we develop for the tactical edge.

Q: OK. Thank you very much.

LT. WALKER: OK. Thank you.

Jared, do you have anything else?

Q: Yeah, sure.

Giorgio, you mentioned a second ago that social media services are more of an OPSEC than an INFOSEC problem right now because people are on separate networks doing this stuff. But that's not going to be the case for too much longer, right? I mean, even at this conference we're hearing about connecting essentially COTS smartphones to the GIG in some -- in some form.

MR. BERTOLI: That's --

Q: So can you get out ahead of those risks or is it just a matter of accepting some risks.

MR. BERTOLI: Well, I mean, eventually, if you're going to allow social media, you're going to have to accept some sort of risk, right? But just because they gave you a phone -- like for example, this is a, you know, government-issued BlackBerry. It's got a camera, but I can't use it; it's turned off. It's got Bluetooth, but I can't use it; it's turned off. So just because I give you a phone doesn't mean I'm going to allow you to do everything I -- you want to do on the phone. So I think it's going really a policy decision as to how much risk the Army is willing to assume providing email and social media to whatever device I have to give to the soldier, as opposed to a dedicated device.

But even that whole concept, right, there's debate between the offensive and the defensive guys, right, as far as what are implication of giving a phone to everybody. Even that -- I think that's actually scarier than the social media -- (laughter) -- concept, right, because there is definitely implications there as far as security goes.

MR. LUCAS: Even right now with the -- you know, the security models for the BlackBerry, it's still a centralized approach, OK? You have a centralized authority that pushes down the security policy --

MR. BERTOLI: That's right.

MR. LUCAS: -- to these devices. When you go to a smartphone, OK, they're going to want that security built right in, OK?

Is it going to be good enough to tie to our high side networks and allow -- you know, basically an unclassified user to tie through our high side network. A lot of analysis needs to be done for that.

Q: What's the answer? (Laughter.)

MR. BERTOLI: I don't --

MR. LUCAS: Well, we're looking it right now.

MR. BERTOLI: Yeah, I don't think anybody knows. I mean, there's lots of issues. You know, I mean, from the cellphone point of view, you know, the concept is sound. I mean, you can't argue with the idea, right? I mean, a lot of times you have a soldier on the battlefield and a cellphone -- a guy with a cellphone -- a civilian with a cellphone can talk and he's got a military radio and he can't, right, because of the geometry or whatever.

And so you have to understand the -- I mean, the concept is definitely valid, right? Why don't we just give them a cellphone? It seems to be working better than the military radio. But there are lots of problems there, right? I mean, how -- you know, cellphones are, you know, obviously exploitable and also, you know, do you use the civilian infrastructure that is there? How much do you trust that service provider in the country that you happen to be fighting in?

All those are serious implications that you have to really think about. Some of those questions just haven't been answered yet.

LT. WALKER: OK, thank you.

I have a couple of questions to follow up with some of Mr. Selby's -- have asked. What does the research and development landscape look like in regards to federal wireless networks, to include cellphone infrastructure?

MR. LUCAS: We actually have an ongoing effort within CERDEC. It's called MACE, Multi-Access Extension for Cellular Environments. And that's actually looking at developing a -- it's basically an applique that would -- that would tie to existing commercial mobile base stations -- cellular base stations -- to provide those unique types of Army-specific capabilities that are needed, say, at the tactical edge. For instance, one would be multicast communication. OK. What I mean by that is, because of our limited bandwidth types of links, the Army tends to broadcast out messages across these links. So it's a one-to-many types of -- type of communication. You don't get any acknowledgement back from the user that they actually received it, though you always hope that they get it. But it's very -- it's a very efficient protocol, OK. It doesn't use up a lot of our resources on our comlinks, still allows you to pass the other critical information that we need to pass over those types of networks.

LT. WALKER: OK. As a follow-up to that, do you have a -- is there currently under development or is there currently available a way to -- you know, we talked about the dichotomy of a military radio that allows for encryption of voice and then, you know, if we were to go to the cellphone technology, do you guys have under development a cellphone encryption device that would mirror that of a military radio?

MR. LUCAS: We're actually looking at a lot of different types of techniques that we could apply to the -- to the commercial-based smartphone types of devices, whether they be Android or iPhone.

A lot of -- a lot of the problems stem from -- you know, you want to try to leverage this constant refresh on the commercial sector.

The problem is when we want to apply such technologies as cryptography to these phones, depending on the level of cryptography, there's a lot of certification or rigorous processes that are applied to certifying these encryption capabilities on these devices.

So the problem is every -- you know, even though I apply, say, a -- or develop a cryptography capability for a specific smartphone, if the vendor, say, a year down the road changes the design of the phone, OK, the physical platform may look the same -- now if I want to continue using this cryptographic device with this phone, I now have to go and recertify the -- you know, the cryptography used with this phone.

And that is -- in itself, is a(n) 18 (-month?) to two-year process every time.

So until the policy and doctrine catch up with us wanting to push out these technologies a lot faster, it's going to be hard for us to interject these technologies quickly. But this is what we need to do to keep up with our adversary. You know, they don't have the constraints that we do.

Q: (Thank you, sir ?)

LT. WALKER: OK, thank you. And my follow-up to that is, do we currently have a system that will maintain our current level of wired security on wireless networks? And that goes for, you know, tablets, cellphones and, you know, just your standard laptop wireless connection.

MR. LUCAS: I think really the only thing out there now is the - is the BlackBerry type of analogy. Giorgio?

MR. BERTOLI: Yeah. You know, I guess the point I would like to make is I have -- I've actually -- I have every confidence in my (C&D ?) counterparts here that from the user level, right, they'll find a way to encrypt user-level data. Right? So I do not fear that somebody is going to be able to snoop in on a soldier's conversation. That is not my worry.

My worry still relies on the fact of how much do you trust the service provider. Right? That, I think, is the critical gap that we haven't figured out yet because, let's face it, encryption -- you can only push it down so far. The protocol that the phone uses to communicate and to interact with the service provider, those cannot be encrypted. Otherwise you're just not going to be able to talk to the cell tower, right? And a service provider has a lot of insight as to what is going on on their network, to include being able to geolocate every single phone for 911 purposes. So how much do you really trust that service provider to potentially even not turn the switch off when you need it most. Right? So that is -- I think is a gap that we're struggling with. The end device, I'm pretty confident we're going to be able to solve that problem.

LT. WALKER: And do you guys have a timeline for that? Do you know when the average user, you know, the average federal worker or the, you know, soldier, sailor or airman, would be able to see some of that technology change, you know, in order to use commercial systems on a military network?

MR. BERTOLI: It would be a guess. I mean, there -- the Army is definitely moving forward with the idea. But there are no timelines that I'm aware of as far as when the first soldier will be deployed with a phone. But I -- you know, a good guess would be probably in the next five years or so would probably -- if it works.

MR. LUCAS: Yeah, I wouldn't even -- I wouldn't even know.

LT. WALKER: OK.

MR. BERTOLI: Yeah. But that would be my best educational guess is, you know, say, five -- the next five to 10 years, should we be able

to solve all these issues -- and there are ideas out there of how to do that -- then you could see this kind of technology being deployed.

LT. WALKER: OK, thank you.

We'll head back around to Tom.

Q: No, ma'am, I'm done. Thank you.

LT. WALKER: OK. Zach?

Q: I'm done as well. Thank you.

LT. WALKER: Dale?

Q: Thank you very much.

LT. WALKER: OK, Jared?

Q: Sure, why not. (Laughter.)

MR. LUCAS: Aw, we were on a roll.

Q: No, quick -- as far as the commercial refresh and keeping up with security, might we get to a point where commercial refresh is keeping up with the security that we need? In other words, like there's no technical reason, right, why HTC can't build a handset that's 140-2 compliant for everybody, and encryption is in place for everybody that meets your standards. And commercial users are going to want security too, right?

MR. BERTOLI: Yeah, but there are issues, right? I mean --

MR. LUCAS: Right. The issue is if you're going to use it in, you know, what we call an unclassified environment, OK -- say, between squad members, OK, roaming out there on the battlefield -- OK, all that information is highly perishable, unclassified for the most part. That level of encryption will -- will probably suffice. OK? The problem is when you want to interconnect to our secret (hide ?) networks, OK? Once you do that, then the National Security Agency has purview over, you know, what's the right level of cryptography in that. OK?

And again, a lot of the -- a lot of the policy and doctrine issues currently prohibit a lot of the FIPS types of implementations to interop with those hi-fi networks, OK?

So you need -- you need the very high robustness encryption algorithms right now -- we call those type 1 base, OK? -- to interoperate with those types of networks.

MR. BERTOLI: Yeah, I mean those, as far as I know, are not commercially available.

MR. LUCAS: (Inaudible.) They're not (released ?). They're export (controlled ?); they're classified.

MR. LUCAS: Yup.

Q: All right, I'll shut up.

LT. WALKER: OK. Thanks, Jared.

I have one other question, and then I think we'll wrap it up. You referred to a common code base. Is the common code base that you referred to limited to one system, i.e., you know, Apple proprietary software or, you know, Mac -- or I'm sorry -- or a Windows-based system?

MR. BERTOLI: No, we tend to -- we tend to leverage higher-level languages like Java, Python, that kind of stuff, just because we don't want to be stuck with a particular way. So we like the portability those languages provide.

So when we -- when we do things like graphical user interfaces or communications infrastructures to -- that become leveraged over and over again, we tend to write in those languages just so we avoid the portability problem.

LT. WALKER: OK, I'm sorry, I do have one more. So if the average person would want to see what you guys do, is there anything tangible that we can go look at online, or is there a current project you have under -- you know, under way that we can, you know, lay our hands or eyes on?

MR. BERTOLI: It would be tough to do unclassified.

LT. WALKER: OK, I think that's it. Does anybody else have anymore questions? (No audible response.) All right, I'd like to say thank you to everyone. We've had some great questions and comments today. And as we need to wrap up today's call, I'd like to ask Mr. Bertoli or Mr. Lucas if they have any final comments.

MR. BERTOLI: No, thank you, everybody for your questions. We appreciate the time.

LT. WALKER: OK, thank you, gentlemen.

Today's program will be available online at the Blogger's Roundtable link on dodlive.mil, where you'll be able to access a story based on today's call, along with source documents such as this audio file, print transcripts and biographies. And if there are any questions about this program, please contact us at newmediadma.mil.

Again, thank you, Mr. Bertoli and Mr. Lucas and all of our blogger participants. This concludes today's event.

END.