

Gen. Kevin P. Chilton  
Commander, US Strategic Command  
February 26, 2009  
Orlando, Fla.

Thanks, General Dunn, appreciate the warm introduction, and yeah, every time I smell Florida, I think about leaving the planet, I'm not sure why that is. But it is really great, as Joe said, to be down here in February, especially when you hail from Omaha, Nebraska. I'm really appreciating the weather. Good afternoon everybody, and a special welcome to a lot of great friends that I see here today; commanders, distinguished visitors, members of our industry team, of course members of the Air Force Association which is such a great support for our United States Air Force, men and women of the United States Air Force, and a special welcome, recognition to the ROTC students from the University of Central Florida. I tell you what, I can honestly say it'd be great to trade places with them and start over again because what they have in front of them in the exciting days that lay in front of them that this great Air Force and the opportunities that are going to be provided them are just going to be mind-boggling, I'm sure in the next 30 years to come. How about another round of applause for those great young folks. (Applause).

It's really a pleasure for me to be here to represent the men and women of US Strategic Command. I'd kind of like to talk a little bit about what we've been doing this past year and what our focus is for the coming year. And over the past year what we have been focusing on, first of all, when I first took command, was to get us a little focused closer on those parts of our missions which require us to conduct day-to-day operations. I call them our three lines of operation, and they are in the mission areas of deterrence, space, and cyberspace. And over the last year we've put a lot of emphasis on these three areas, and our component commanders, which we have in each one of these; for space, deterrence, and cyberspace, have executed their missions exceptionally well with the joint forces assigned to their organizations.

They're focused on conducting missions every day and so is US Strategic Command, because those missions that we conduct are absolutely critical to the war we're engaged in today, and in a broader sense, they're critical to the security of the United States of America. We've made a lot of progress in this past year, and we do have some work here ahead of us. I would like to speak a little bit about our progress, and let me start first with the deterrence mission area.

Obviously coming into command in October a little over a year-and-a-half ago, there was no doubt in my mind where we needed to focus our first bit of attention and that was in the nuclear area. And we have done that over the past year, and I think we have made great strides as our United States Air Force. At STRATCOM, we have worked to strengthen our ties with our Nuclear Task Force Commanders, in both the submarine task force, the airborne command and control task forces,

and the three critical Air Force task forces we have: 204, 214, and 294 are commanded by General Elder and General Berg and General Skip Scott. Our bomber, ICBM, and tanker task forces have really turned too, and that closer tie with the headquarters at US Strategic Command has provided me the insight that we need every day into the status and readiness and preparedness of our nuclear deterrent component to do their job.

Additionally, General Elder has taken on the mission set for US Strategic Command to try to figure out how we are going to implement the concepts of deterrence which have not changed, but the applications will change in the 21st century, how we operationalize the concepts of deterrence in the 21st century against the various foes and potential adversaries that the United States may have. But it doesn't stop there--internal to US Strategic Command, we've rebuilt our IG shop, and today, every nuclear inspection that's conducted in the United States Air Force or the United States Navy has a USSTRATCOM IG member attending that inspection, whether it's under the sea, in the missile silos, in the airfields, or in the command and control elements, USSTRATCOM is there and they report directly back to me the results of those inspections, the quality of those inspections, the consistency of those inspections, and any trends that we may be observing in those inspections.

We moved a flag officer position into the headquarters of J-3; General Joe Brown, United States Air Force, has recently arrived to fill that position. His one focus area is the nuclear mission set--100 percent, 24 hours a day. Joe Brown is paying attention to that mission set for our J-3. Additionally, we've stood up a nuclear enterprise ward and a nuclear enterprise council, which Joe puts together the teams to brief, and is overseen by my deputy commander Vice Admiral Mauney, and Van's job is to keep a broad overview and scope and understanding of all the programmatics, logistics, soup to nuts, that could affect the readiness of our forces today, as well as looking into the future to make sure we're postured appropriately.

We've taken steps to begin to rebuild our intelligence support, our J-2 shop at the STRATCOM headquarters, which had been drawn down in the past to allow us to answer some of the key questions that are essential for not only the deterrence mission set but for space and cyberspace. Today, flag officers are back on alert for the (inaudible) mission. Our crews are no longer sitting alert for a mission that requires a flag officer without a flag officer at the ready. The United States Navy is pitching in, but the United States Air Force is pitching in a very, very big way, and I thank the Chief for his support of this program. The number of general officers that have volunteered and come forward and are re-qualifying I think is a win-win, both from US Strategic Command as we send the signal that we are serious about this mission, and for the Air Force to get better understandings and go back to the future, if you will, clearer and better understandings of what it takes to conduct the nuclear deterrent mission.

I salute the Air Force and I salute Chief Schwartz and I salute General Kehler and (inaudible), my friend, for the emphasis that you have put on at ACC and Air Force Space Command on the nuclear enterprise. I think we're seeing tangible and real results and readiness and I can tell you today, as I can tell both friend and adversary, that our nuclear forces in US Strategic Command are ready today to do their missions at the direction of the President of the United States. We've taken another look at our exercise programs at STRATCOM and we're moving away from command post exercises to FTX, force exercises. And I'm very much excited about Global Thunder, that's coming up in June of this year, where we'll get a chance to see the Air Force shine, and particularly 8th Air Force, with the bomber mission, and also Task Force 294 with the tanker mission.

As I consider the nuclear mission, I think it's important for us on occasion to step back and remind ourselves of all the major piece parts or components that are necessary to successfully provide a nuclear deterrent for this nation. What does nuclear deterrence require? It's a pretty short list, but an important one. First, it requires warning systems; both ground-based radars and space-based infrared warning systems. It requires reliable communications systems so that orders from the President can be transmitted to forces in peacetime and at the height of conflict. It of course requires reliable people that are trained and ready to do their mission, and it requires reliable delivery pod forms--submarines, ICBMs, (inaudible--ab and caps?), tankers, bombers. And of course, none of that is any good if you do not have reliable weapons with high margins of performance to ride in or on top of those delivery platforms.

Today, as I reflect on each one of these needs to provide the nuclear deterrent, I begin looking at the weapons that are required. And today, as a year ago, we still have a lot of work to do to improve the infrastructure in the United States of America that is required to support the sustainment of the nuclear weapon enterprise. We need to continue to work to attract the right talented people to enter this enterprise to ensure that we will have that capability sustained for decades to come, and I will point out again, that of all the declared nuclear-powered nations in the world, the United States of America is the only one that is not currently undertaking a modernization program for their weapons. This is something we must address and I'm confident will address in the coming year as we look at the MPR.

When I think about people and I think about our delivery platforms, both of them need to be inspected closely and exercised in difficult scenarios. And again I want to compliment the Air Force for raising the bar in the way they inspect nuclear forces. There's been some criticisms out there recently in the press about failures. I appreciate the increased scrutiny, I appreciate the increased focus and attention, and as I said before, I oversee and analyze the results of these inspections, and I can tell you today, our forces are trained and ready to do the mission. And I'm very proud of what the Air Force has done and what the US Navy has done to put me in a position to be able to stand up here and tell you that

today.

When I think about reliable warning systems and communication pathways that we can count on in time of crisis I have a little bit of an uncomfortable feeling, not for where we are today. We have excellent systems in place today, but as I look to the future and I look at our plans and our programs for the future, I worry that we have gotten into the mindset or have become accustomed with the mindset of "just in time, re-supply" of critical on-orbit constellations is good enough. In fact, I think we have almost gotten to the point where we are counting on in our architects and planning and delivery schedules for 100 percent launch success. Now, I got to tell you, when I hear someone counting backwards from 10 I naturally get a little nervous myself. It's bad enough to watch a launch because they're such an exciting thing, and you're hoping for success for a launch, but to have to watch a launch and know that if it fails or if that satellite fails to reach orbit, you're going to create a critical gap in what this nation needs for warning or critical NC2 communications. That's a different level of worry. We don't have the problem today, but actions that we take today and the way we approach our critical space constellations today will matter 10 and 15 years from now. I think it's passed time for us to change the way we think about keeping these constellations populated. Managing to a gap is not the way to go; having a little robustness, having the ability to sustain a launch failure, is something that we should very much consider as we look to the future.

While I'm on the topic of space operations, JFC Space, under the leadership of General Willy Shelton and now under the leadership of General Larry James, has done just an absolutely fantastic job over the last year. This is another area where we need to continue to maintain the momentum that we've achieved over the past year in 2008. It's hard for me to believe that it's been a year since I stood on this platform and was able to come here I think the day after the successful intercept of the defunct NRO satellite by the US Navy SM-3, Operation Burnt Frost was a year ago, ladies and gentlemen. I'm very proud of what the STRATCOM team accomplished in that effort. I'm also equally happy to report to you that every bit of debris created by that intercept has de-orbited today, just as what was forecast, and just as we considered in our planning and executing of that mission.

But the debris situation on orbit has gotten worse in total. I think that when I came back from NASA in 1998 to Air Force Space Command we were cataloging and tracking about 8 thousand pieces of debris or objects on orbit. Today, it's 18 thousand. The trends are not in the correct direction, and as was highlighted here recently with the collision of an active satellite and an inactive satellite on orbit and their creation of additional debris, it's something that we cannot take our eyes off of. The increase of the debris, the fact of the collision earlier this month, highlights the fact that we have more work to do in this particular area of developing adequate space situational awareness to provide warning and support not only to the critical systems that we think about today in space, which might be our intelligence collection platforms, our communication platforms, our

manned platforms, but also expanding that capability to consider some of the key commercial platforms that our operations rely on today in Iraq and Afghanistan; the commercial bandwidth that we release through commercial satellites that support our Predator operations, our GlobalHawk operations around the world. Today we don't have the capacity to provide the conjunction analysis, which is space words for collision analysis, for all the things that we would like to do. And this is an area that we can and will make advances in in the coming years and Air Force Space Command, the leaders there got the picture. They have the vision; they just want it faster, and I want it to happen faster for them. They're doing a super job out there.

I applaud General Kehler and I applaud Mr. Scott Large from the NRO for paying attention to another key part of our space requirements, and that is the formulation of a group called the Space Protection Program, that is going to take a good hard look at our critical satellite capabilities, and how we can robust those constellations as we look to the future; how do we need to change requirements for the development of those constellations. So we finally start thinking about fielding systems on orbit that go beyond just executing the mission, that are also focused on protection of the satellite and the constellation themselves.

Now, if our theme is sustaining this great momentum in the deterrence area from 2008 into 2009 and sustaining this great momentum that we've achieved in the space area in 2008 as we come into this year my message for the cyberspace mission is it's time we generate some momentum in this particular area, and it's going to be one of my high priorities as we move forward in 2009. It is indeed becoming a major focus area inside US Strategic Command. You know when I think about the challenges in cyberspace I'm reminded of a joke, a story about Sherlock Holmes and his sidekick Watson; how after a tough week in London decided to go out to the countryside for a little relaxation. And after a fine meal, an evening around the fire, they retired to their sleeping bags for the night. About 2:30 in the morning, Holmes woke up and he nudged Watson and he said, "Watson look up, tell me what you see." And Watson said, "Why, Mr. Holmes I see a most magnificent sky filled with stars and planets." And Holmes said, "Well what does that make you think? What do you deduce from this?" He says, "Well, it makes me wonder at the magnificence of the galaxies, the network of stars that are up there. It makes me wonder about our place in the universe. And how about you, Holmes? What does that make you think?" And he said, "It's elementary, my dear Watson. I can deduce that someone has stolen our tent." (Laughter.)

Sometimes the obvious can sneak right passed you. In the cyberspace domain, here are some obvious things: We are under attack. We are behind. We are reactive; we are not proactive. And, we, all of us, are making it too easy, too easy, for those who would exploit and attack our networks today. I think there are three areas, general areas, where we need to make some improvements in this particular domain, warfighting domain. They're in culture, conduct, and capabilities. Think about our culture and how we culturally think about

cyberspace and use it. Well first you kind of look back in the rearview mirror how it grew up. It grew up as technologies that sprung up in different places--writing on the Internet, creative applications developed by young smart lieutenants or NCOs in your organization, new capabilities, new off-the-shelf things built in, kind of controlled and organized and thought about at the local level and not really at the global level. When you had a problem with your computer, who did you call? Your information manager, who used to be your admin clerk back in the days before computers. And if he couldn't solve it or she couldn't solve it, they called the communication folks inside your organization.

I ask the question--do commanders today of our wings pay attention to the health and security of the networks that they rely on to conduct their operations? When I was a wing commander, we used to review the maintenance statistics every day to check on the ability of our airplanes to do their mission. Guess what? Today those airplanes can't do their mission if we don't have a protected cyber domain to protect scheduling, the movement of orders, the transfer of information, the movement of ISR data, etcetera etcetera, required to conduct those operations. Cyberspace is not CICS business, it is commanders' business, this is a cultural shift we need to make, all of us. Commanders need to be demanding of their CICS, what is the status of my network? How compliant are we with directives for the defense of that network? And it should be just as important to commanders as the MC rates or all the metrics we look at for logistics and maintenance on our aircraft. Commanders should demand reviews of the health and status of their networks.

We need to recognize, another cultural shift, that a vulnerability in one machine is a vulnerability to the globe, not just to the local office space, wing headquarters, base, or AOR. Every computer can be a portal for the adversary to come into our network and either steal information or create havoc in time of increased conflict.

Another cultural thing I think we have to adjust fire on is the way we use our computers, particularly the Nippernet everyday at our desks. Do you know we afford more protection for the little black pens that say "For Government Use Only" than we do to the computers on our desk on what we allow people to do? We need to change our mindset of those computers, the Nippernet machines, from being a convenience to the way we do work, to being absolutely critical to the mission, and have a mission use only mindset and culture for the use of the Nippernet. Change in culture doesn't happen overnight, but it starts with leadership, and it starts with commanders talking about this.

Now shifting to conduct--there's a lot we can do as leaders in the way we conduct ourselves and conduct our forces to adjust things in the cyber domain in a positive fashion. For example, one thing that we're very accustomed to is inspections--ORIs, NSIs, commanders prepare for them, IG teams prepare to give them. We peak for them, we're ready for them, we exercise and train to

accomplish them, and when people come to inspect us, they expect us to be able to be ready to do our mission and they expect us to be compliant with directives from our headquarters. We need that same level of inspection rolled into our inspection process for the cyber domain. So when the IG shows up to check whether or not your bomber can man up, load weapons, arm up, meet the maintenance generation requirements, they also need to be inspecting whether or not your installation is compliant with directives on how to secure your network, and you should be graded on that. That's a change in conduct that will help change our culture.

Training--I don't know about you all, but I'm required, I'm sure you all are too, once a year I get a message on my computer that says, your annual IA training is due. And I do it, as I'm sure you all do, and it's a pretty darn good little lesson. Once a year; what kind of message does that send about the criticality of this? When I was flying RF-4s as a second lieutenant, we had daily threat and Intel briefs about the threat that we were facing, and that threat wasn't changing very much--MiG-15s, MiG-17s, MiG-21s. The threat in cyberspace is changing every day, and yet we don't have a conduct or a culture that informs our people what that threat is, how to recognize it, what's the latest phishing threat that's out on the Net today, do you know Airman Chilton, because you're on the Net? We don't have that in place. I think we need to increase the amount of training we provide for our people and our visibility (inaudible) into the threat. Cyberspace, to be effectively defended and operated, demands centralized command and control. People don't want to accept that because of the way cyberspace grew up inside our individual post-camps and stations, but if we're going to get this right, we're going to have to exercise that centralized command and control.

Never more evident to me than this past year when I asked a simple question--how many Sippernet machines do we have and how many Nippernet machines do we have in the Department of Defense? Now if I asked the US Air Force how many pistols or how many rifles we have, certainly if I asked the Army I know this to be true probably within 24 to 48 hours someone would be able to tell me how many we own and probably where they all are because they're manually logged in and out of every armory in the United States Air Force and Army. And if we didn't do that correctly you know we run the risk of losing track of a firearm that could kill somebody in its immediate vicinity. It took over 45 days to get the answer to how many Sippernet and Nippernet machines are on our networks because of barriers put up by individual organizations, refusal to respond to direction, architectures and technical limitations that prevented us to go down and find out the answers to these questions. The next question was; What configuration are they in? Have they got the latest software updates on them, etcetera, etc. etc.? We need to be able to do that at machine-to-machine speed, and until we can, we need to have a command and control system in place, commanders in place, who understand their responsibility, and react to the orders given by the JTF for Global Network Operations.

Another thing that I think we can change in our conduct that would be beneficial and I've seen the Air Force start to do this and I applaud Gen. Schwartz for it, is to implement a kind of mishap investigation, if you will, for when we get broken into it. I mean we go through excruciating pains to learn lessons from aircraft accidents. When we have tremendous amount of sensitive data or information taken from our networks, do we do the same level of investigation today? Should we? Should we disseminate lessons learned from that? We absolutely should. These are changes in conduct that I think are essential.

Now let me transition to capabilities. We owe our people better tools, and we need to make the appropriate investments so that we can achieve this vision of being able to manage and defend and operate the network at network speeds, machine-to-machine speeds. I don't know about you all but my computer home, my personal computer, every time I turn it on and log on some banners come up, says, "We've just run the anti-virus scan on your machine, the latest anti-virus has been updated." You know you can bet my Internet service provider knows when I'm online. We don't know when our people are online necessary. They need to know because it's a business case for them. We need to know because it's mission essential, it's bigger than a business case. We need to be able to push software upgrades automatically just like I can get at home on my computer. We need to be able to put warnings out automatically so that when our people log on they know what's going on on the network. The Host Based Security System, HBSS, is a program that can help us move forward in this particular area, and I'm happy to see that the services are putting emphasis to pull the readiness and deployment of that program back earlier with a vision of having it totally deployed by the end of this year.

We also need common operating picture in this domain, no surprise. You need them in air, you need them at sea, you need them in space, we need them in cyberspace. Today if you look at the JTF-GNO common operating picture for the Nippernet and Sippernet and you zoom in on some locations around the United States you'll find black holes because we don't know what's going on in there because firewalls have been put up by organizations, connectivity has not been made available, we have not understood and moved to the point where we understand the need for centralized visibility and the ability to push updates, patches to software, etcetera.

And finally, in the capabilities area, what we need are people. We need trained people that not only know how to do the exquisite things that you read about, people talking about, dreaming about doing in the paper of the attack and exploitation area, we need people who are trained on how to operate and defend these networks as well. We need service forces, we, US Strategic Command, need service forces that are organized, trained, and equipped and presented to this combatant command so that we can conduct the missions the President of the United States has given us--to operate and defend and be prepared to attack across the network. Culture, conduct, capability: I'll be talking about this all year

at US Strategic Command, and we're going to need a lot of help. We need to work this together as a team if we're going to get out from being behind, if we're going to ever get out from being reactive and move out on being proactive in this domain.

I noticed the theme for this conference is cross-domain integration, and I think that's spot on. I tell you that's an area that we work really hard at US Strategic Command and we have a long ways to go. When I think about our three main lines of operations and our global responsibilities, I try to translate into a reasonable combatant commander's responsibility and his three lines of operations. His are: air, land, and sea. Ours are deterrence, space, and cyberspace. Think about the power of integration of air, land, and sea in the joint force. That integration happens when those component commanders work tightly together to achieve the combatant commander's intent and objectives. We have sought no better demonstration of this in my view than Operation Iraqi Freedom when you looked and saw how Phase III of that operation unfolded, and the close-knit operation and planning that was evident between the air, land, and sea component commanders and their teams for the kick-off and execution of that operation, it was absolutely brilliant.

We have that opportunity in USSTRATCOM today to integrate space and cyberspace and deterrence operations in such a fashion to bring a capability that's better than the sum of its parts to the fight, and a capability not only for meeting national security objectives but a capability that first and foremost and most likely is there to support the regional combatant commanders in time of crisis. We do that today with our lines of operations and we're proud of that. We can move the ball further forward in this area, and it's going to be a focus for US Strategic Command this year. How do we better integrate internally, and then how do we better integrate our capabilities into the fight in the regional combatant commands? The thought of breaking apart this synergy of deterrence, space, and cyberspace global mission sets makes about as much sense to me as breaking apart air, land, and sea components in a regional combatant commander. I think we go down that path, which I think sometimes there's temptation to do, we will miss the opportunity to increase and find the synergy that is there inherent in these global mission sets.

Well in addition to our focus on our three lines of operation, we have just a few other things on our plate at US Strategic Command. This year we're going to continue our efforts in supporting and planning and advocating for global missile defense, for ISR assets, for all the combatant commands, for countering weapons of mass destruction, and planning to develop IO capabilities and advocate for them, that will also support combatant commanders in their fight, as well US Strategic Command. Not to mention a few of my favorite acronyms that are on the charts--POM, POM, QDR, and oh, don't forget, NPR, a very important year for NPR, a very important year as we re-look at our nuclear posture for the future and an area in which STRATCOM and the Department of Defense is going to

need the help and advice of the key services, the United States Air Force, the United States Navy, as we move forward in this area.

But I assure you, in spite of all of these three-letter acronyms, our overriding focus will remain on our three lines of operations. We'll continue to look at how we can better integrate those operations between each other and how we can better integrate them into the fight, and how we can bring them to bear every day as we try to do today to support every COCOM on the planet; ultimately to ensure what we are about at US Strategic Command, and that's providing global security for the United States of America. Ladies and gentlemen, thank you very much for your attention. I look forward for your questions. (Applause.)

Dunn: Thanks, General Chilton. Because our Chairman of the Board used up so much time in his introduction, we only have time for just a couple of questions so if you don't mind.

Chilton: I planned it that way, Mike.

Dunn: A little bit on the Nuclear Posture Review, there's a lot in the press about large cuts in (inaudible) warheads, in de-alerting ICBMs, ratifying the Conventional Test Ban Treaty, and lots of other ideas. Would you care to comment on any of these ideas in general and in terms of your own thoughts?

Chilton: No. What I would comment on, Mike, is that I think the right way to go about this and I think the way it will be addressed, I'm sure it will be, is, you go-- what's our policy? What's our strategy? What's the force structure we need to execute to support that strategy? You don't start with a number and back into a strategy, in my view, and that's what the QDR should be about, and will be about, is asking the key policy questions and then strategy questions, and then examining those as you bounce back and forth between multiple options on the impacts to deployed forces, force structure, etcetera. That trickles right down into industrial base issues, etcetera, so it's a broad area that quite frankly, it's time to dive back into, and dive back into in a serious way.

Dunn: Thank you. On the cyber world, you talked about what we need to do as DOD and the services and we are under attack, as I read the press; Kyrgyzstan, most recently, of course Estonia, the country of Georgia, the Pentagon, there were a number of these attacks that have been prosecuted, and you talked about the focus going forward. What kinds of larger policy questions do you need answered, in other words, what comes to mind is; what constitutes an attack? How do we treat certain incursions? What happens if somebody takes down certain things? Are there national policy decisions that you would like to see addressed going forward?

Chilton: I think the question of what constitutes an attack is one that probably warrants some discussion, and when you cross a threshold there, I think that can

be fleshed out in games and exercises with senior leaders, to understand, where have you crossed the line that your response might be something other than in cyberspace, which it doesn't necessarily have to be. It could be in another area. When do you start applying, based on what's happening on your networks, when do you start applying the other elements of national power, and how and when? And so, what are your trip wires for that? There's another important part of that, too, when you think about deterrence--what are the positions that we want to take openly to send a signal of what we will not tolerate, or place ambiguity in the mind of an individual or a nation-state that might think about attacking us in this particular area. I'm reminded of, back in the early 90s, an article I read in the newspaper that said, Russia had come out and said that they would consider an attack on their computer network systems as an equivalent to a nuclear attack, and they would reserve the right to respond accordingly. And I thought, wow, that's some red line. It was about two days later they retracted that. But I mean, so you got to think through, in the deterrence area, obviously someone was trying to deter somebody there. It wasn't very credible, which is part of deterrence, how we're going to think about this particular domain in that scenario?

Dunn: Last question and it's a very simple one. You did mention that we are under attack--I'm not sure the general public realizes the trends in terms of any kinds of measures that are available and where are these attacks coming from? Are they going through various countries, or is it country-related, or is it individual-related? Can you give us any information on--?

Chilton: Well, the threat comes from as far on one end of the spectrum from what I call the bored teenager, to the other end, a highly sophisticated nation-state. And then in the middle you can find some pretty highly sophisticated folks, too, and a criminal element there too, is interested in taking the money from your bank account, from your personal computer for example, or breaking into financial systems, whatever. It's hard to say how much of that is going on because quite frankly when financial systems, at whatever level, may experience some kind of interruption or attack, they're not particularly interested in advertising that. There's a cost of doing business out there. The question is, when do you trip that over? Clearly in our case, in the Department of Defense, there's no doubt that we are being exploited in this area, and information is being taken from our Nippernets, and our unclassified networks, that when combined and put in total, can be used against us, and in particularly in time of conflict; can be used to understand how we think, how we operate, etcetera, vulnerabilities.

And as to where these attacks come from, this kind of pulls back to the idea, to the notion, that this is a global mission set because the network runs around the globe, and so attacks may originate in one area of the world and use servers and nodes and entry points from all over the world, which brings you back to situational awareness and attribution, the power of situational awareness and understanding not only the status and health of your network but being able to attribute an attack on your network so that you then can turn to the President

and say, this is what happened, this is who did it, what elements of national power would you like to bring to bear to address them?

END TEXT