General William L. Shelton
Commander, Air Force Space Command

Air Force IT Day
AFCEA NOVA Chapter
Defining the Future of Air Force Cyber
(As Prepared)

11 December 2013

Chuck, thanks for that kind introduction, it's nice to be here again. And Chuck…thanks to your host of volunteers who have worked behind the scenes over the past few weeks.

General Hobbins and General Keyes, it's great to see you, and thanks for being here today. I'd also like to thank the NOVA Committee members who bring this audience together to discuss some important issues during a tough time.

It's always challenging to speak to such a diverse audience, one that understands implicitly how important our space and cyber capabilities are for joint warfighting and for our economic well-being.

And I think this audience will agree, space and cyber capabilities have changed the form of modern warfare…and they will become more important over the long-haul…as such, we have to ensure they are preserved.

As Secretary of Defense Chuck Hagel recently acknowledged, "*As our potential adversaries invest in more sophisticated capabilities and seek to frustrate our military's traditional advantages, including our freedom of action and access, it will be important to maintain our decisive technological edge.*"

I completely agree with the SecDef…we must maintain our edge…our Nation can't afford to surrender our lead in space and cyber.

But I don't want to focus my comments today on the budget issues. Quite frankly, I'm tired of thinking about it, tired of losing sleep over it, and tired of living it.

So, instead, I'd rather talk about a much happier subject: what our AFSPC Airmen are doing to lead the way, helping to ensure our Air Force remains the greatest air, space and cyberspace force in the world.

I'll talk about cyber, what my command is working on today and into the future. I'll be jumping around on several different subjects, so please hang with me.

And of course, I'll leave a few minutes at the end to hear what's on your minds.

So let's start with what I assert as a given -- space and cyber capabilities are absolutely foundational to America's future…our military, our industry, our freedom of action…you name it…they touch everything.

Militarily, space and cyber capabilities enable seamless command and control, global surveillance and precision targeting, among many other things. If you think about it, our Air Force has been at war for nearly 23 years, starting with Northern and Southern Watch, right through Desert Storm.

During that time we've stitched space and cyber into the fabric of joint operations and created a synergy that has changed modern warfare. Our own mental model has shifted, as planners now actively consider the full space and cyber toolkit.

Our potential adversaries have been watching us these 23 years, and they have gone to school on our space- and cyber-enabled modern warfare. And our dependence on these domains yields a corresponding vulnerability for adversaries to exploit.

I think it's fair to say that without a doubt, they will challenge us in space and cyberspace.

As our dependence has grown, both domains have become increasingly contested. And in cyberspace the threats have grown both in quantity and sophistication -- denial of service attacks, malicious code, direct attack on critical infrastructure, and theft of intellectual capital...these are all serious problems we face.

And as many of you have heard me say before, the price of admission to be a contender in the cyber domain is very cheap…literally a computer, an internet connection and some software savvy and you're in.

The adversaries we face in cyber come from a troubling mixture of backgrounds and agendas -- state sponsored hackers, actors with an ideological agenda, criminals and probably most troubling to patriots… insiders.

The threats are sometimes very obvious and discoverable, and sometimes very insidious and difficult to detect…and we have to be ready for both. Which is why conferences like this are so important--we must be able to operate in, defend, and fight through the challenges in the cyber domain.

To be successful, we'll all need to think very deliberately on how to counter these threats and how to ensure cyber mission accomplishment, even in the face of attacks.

Let me say that a different way: even when challenged, our data MUST get through, it must be timely, and it must be valid. True for C2 data, intel products, TPFDDs, Air Tasking Orders—you name it.

While denial of service is scary, so would be discovery of manipulated data in our networks during conflict. The corresponding lack of trust that would follow would result in much confusion and at minimum, delays in our ability to prosecute the fight.

[TRANSITION]

The Airmen in my command are leading the charge in these areas and working through sophisticated defense methodologies. We're using the standard approach to defense, which starts with Defended Asset Lists provided to us by our users.

And by the way, we can all agree that the cyber domain is a very different animal, but we're increasingly finding that application of tried and true military processes pay dividends in the cyber domain as well.

So, let me shift gears and talk about some things we're doing to try to normalize cyber ops in our AF.

Normalizing cyber operations has been a challenge because as some of you have experienced first-hand, cyber's genesis was disparate networks with inconsistent resourcing and very disparate roles and responsibilities.

Networks grew-up base-by-base with an eye mainly to each base's mission. Eventually, as MAJCOMs took ownership, there was a beginning to enterprise oversight, but it stopped at MAJCOM boundaries. We still had no enterprise, a lack of standards, configuration control and most importantly: zero enterprise-wide situational awareness.

This changed somewhat with the standup of the Air Force Network Operations and Security Center, at Barksdale AFB in 2004…at this point we began to see some centralized vulnerability management and enterprise security.

A great start…but we still had the issue of numerous distinct networks, gateways and program office networks…and we didn't have a good handle on the activities writ large.

Fast forward to today: AFSPC, 24th Air Force and the Air Force Network Integration Center (AFNIC) have worked hard to consolidate all of these networks into a single Air Force Network…the AFNet.

We've collapsed 120 different network entry points into 16 gateways and already improved our ability to secure the AFNet, monitor traffic and provide defense-in-depth. So far we've migrated approximately 90 percent of our 275 targeted sites, which equates to just over 580K users.

We'll be fully consolidated by the spring of next year, and when finished, we'll have a single enterprise network with consistent standards…one that we can defend.

The user experience will be greatly improved: once migrated, the CAC card allows you to access the AFNet from any AF location—just as if you were at your home base machine. And we can begin to think about enterprise solutions for our users to simplify account management and gain efficiencies.

What if: when you got your CAC card at BMT or your commissioning source, your account was created and you didn't have to reapply for an account upon every PCS move? Instead, we would provide a website that would allow you to update your account as needed, but no need to spend extra quality time establishing accounts every time you move or go TDY.

This is but a small sample of what our folks in 24th AF are thinking about, enabled by an enterprise capability and approach.

As we go forward, there are areas where we'll continue to innovate and shape the enterprise. Our teams are looking at ways to weave in commercial and cloud solutions to meet our enterprise goals. We're looking hard at the "Next Generation Desktop"…commercially provided e-mail, data, voice and collaborative tools…unified capabilities which could save millions of dollars.

And, we're looking at integrating technology that will make our workforce more productive…like tablets and next generation mobile computing.

It's no secret that as we envision the future, we have to continue working the "lanes in the road" discussion. In the past, there was no MAJCOM with the lead for cyber, so things defaulted to the Air Staff.

Now, we at Air Force Space Command have assigned responsibilities for both cyber operations and cyber programs. It's really no different from the air and space domain, if you think about it. Let me use the air domain as an example.

If we have capability shortfalls in either the CAF or MAF, whether they be weapons systems or infrastructure, we count on ACC and AMC to define the requirements, work those up through the AFROC and JROC, then work closely with the appropriate product center to close the gap. Why would cyber be any different?

We get a little hung up on definitions of cyber and IT, and getting those definitions clear and agreed upon is absolutely critical, but it turns out we're having a devil of a time reaching consensus.

In AFSPC, we're absolutely focused on providing joint cyber capabilities, which means we have to avoid an IT-minded approach to cyber. Certainly IT provides the great tools and platforms we use, but that *is not* cyber operations…no more so than the F-22 sitting on the ground is doing air superiority.

We have to operate in a domain that's *created with IT* to accomplish cyber ops and produce joint warfighting effects. Additionally, conducting cyberspace operations includes having the tools to do the job…like we do for other capabilities in our inventory.

Earlier this year we made a significant step when our Chief of Staff declared 6 of our cyber capabilities as weapon systems—another big step toward normalization. If that catches you slightly off guard, please understand, these are not weapons in the conventional sense…we used the proven, standard weapon system construct to establish a business process to drive our investments in this domain.

Just as the Air Force must invest in, maintain and sustain our air assets, we're using the standard weapon system framework to source our cyber capabilities. For example, for two years now our Airmen have conducted defensive cyberspace operations for Air Mobility Command (AMC) using the CVA/Hunter system, one of those "weapons systems," that's an active cyber-capability that we've invested in.

It's purely defensive in nature, and it stays within the boundaries of our own network—nothing really "weapon" about it. But the weapon system process and the sustainment discipline and funding protocols that go with it, will help normalize this business.

Now let me shift gears again on you and talk about our contribution to the Joint Cyber Force. And Cyber Mission Teams are where the rubber meets the road in cyberspace.

USCYBERCOM recently established a Cyber Mission Force requirement to conduct full spectrum cyberspace operations…this is where our Airmen will provide vital capability for joint cyberspace operations.

Over the next 3 years, the Air Force will provide 39 distinct teams to CYBERCOM as our share of the CMF. These cyber mission teams will include National Mission Teams, which defend our nation from strategic cyber-attack; Combat Mission Teams, which support mission execution for combatant commanders, fully integrated with operations in all other domains; and Cyber Protection Teams that provide mission assurance and defend missions in cyberspace.

I mentioned a few moments ago that our Airmen are conducting defensive cyberspace operations for Air Mobility Command (AMC)…going forward we will extend DCO capabilities to Transportation Command (TRANSCOM) prioritized missions, meeting the needs of General Fraser and his Command.

When fully operational, we'll have over 2,200 Airmen in 24th Air Force/AFCYBER committed to the Cyber Mission Force. We've already re-cast some of our folks conducting these joint missions.

Next let me talk briefly about some exciting work we're doing with the Army and DISA on the Joint Information Environment.

Honestly, we've spent several months doing some important due diligence on JIE implementation. While our commitment to the JIE vision is unwavering, as the AF lead for cyber, I felt it was important to look before we leapt—and it was some good discovery work by a host of people.

We've now formed a very strong and productive partnership with the Army and DISA and we will begin implementing our Joint Regional Security Stacks early next year….our operational success with our AFNet Gateways has been instrumental to this effort.

We will also provide enclave control nodes for JIE at 10 of our Air Force bases, integrating the Air Force into the JIE enterprise. And the Air Force has leaned forward with classified Defense Enterprise E-mail…or DEE, and while DEE is not part of the JIE architecture per se, it is a step toward the JIE vision of a single DoD enterprise with centralized services.

We're still in a due diligence mode on unclassified DEE, working through the cost estimates with DISA. So we're tapped into JIE and partnering to define the single joint enterprise. As with everything else these days, we are looking hard at every aspect of this transition to ensure we gain the resource efficiencies predicted.

Clearly, combatant commander and warfighting priorities remain the primary focus for all our space and cyber capabilities. And while the United States remains the leading global military power, that status is being challenged every day.

It's imperative the warfighter trusts the data they receive from our space and cyber systems…anywhere around the globe, 24/7. And as I've said, we need to ensure the data gets from Point A to Point B, through any contested environment.

Our adversaries will also use cyber to inject themselves in space, wherever they can, particularly at the seams in our capabilities. Cyber-attacks—to deny command and control of our satellites and by interfering with the Air Force Satellite Control Network…let me assure you, we are very concerned about such threats. Our

adversaries are looking for accessible single points of failure, and we must harden our systems.

A watchword in my headquarters is ***resiliency***…that's where we're headed with future space and cyber architecture. Resilience means that despite adversary action we still have a capability to present to the joint warfighter.

Let me give you one example. The Iridium constellation uses 66 satellites in low-earth orbit to provide commercial comm and data services. The resiliency of Iridium's constellation was certainly tested when a Russian KOSMOS satellite collided with one of Iridium's satellites in 2009. Despite the loss, the constellation was still able to support users because of the overall resilience inherent in the constellation.

In stark contrast, the national security MILSATCOM architecture is nowhere near as resilient.

In fact, with most SATCOM systems, we're often one-deep on capability because it's expensive…we build just enough and just in time. To get to a much more fault tolerant architecture, we're working hard to find the balance between affordability, capability and resilience.

There are a lot of good ideas on the table right now… discussions between staff in my headquarters, industry and the Space and Missile Center at Los Angeles.

In fact, we're wrapping up a study that addresses joint warfighting requirements and resiliency in order to project what our future architecture will look like.

This study is looking at a number of environments to paint the picture. Benign, those with some IO or jamming activity; contested, direct and purposeful kinetic/non-kinetic or

IO attack on our systems; and, nuclear, aimed at protected national critical assets to support senior leaders during and after a nuclear event. [TRANSITION]

For space and cyber, the reality is that we're facing external threats outside of DoD as well as tough budget challenges from within.

For the long term, the ripple effects caused by continued sequestration mean uncertainty and a bow wave of bills that will someday come due. As we continue to make headway in cyberspace, the long-term effects of sequestration will challenge us on many levels. We can't continue with the status quo: business as usual...we simply don't have that kind of money.

But the good news: We are the best Air Force in the world with the best Airmen around…and they're looking at solutions.

We have a lot of hard work ***and*** opportunity ahead of us, but it requires us to find answers to some pretty tough questions. It starts with a team of Airmen, contractors, researchers and industry innovation…good ideas from all quarters.

And speaking of industry, we know that the commercial sector is ahead of the government sector in technology in cyber…so we need to hear from industry. We're putting all ideas on the table, listening to folks from government, industry and those within our command.

On the people part of this, a lot has also changed in how we prepare our people to conduct cyber missions. For one, we've moved to much higher training standards… there are requisite skills our cyber operators need in order to do the mission. And, we expect a level of preparedness from our cyber operators that didn't exist before…they have to be certified to "fly" missions in cyberspace.

And the folks we need in the driver's seat must have the right combinations of tools to head us in the right direction.

It never ceases to amaze me how much talent our Airmen, contractors and industry partners demonstrate every day.

[TRANSITION] We have some challenges AND opportunities ahead of us, so we'll need all the talent we can muster.

Thanks for the opportunity to speak today.

Space and cyber are absolute game changers for modern warfighting.

And the demand clearly exceeds our resources. But that doesn't change the fact we're going to continue to lead at the edge in cyber…our Nation depends on it.

I look forward to where we're headed as an Air Force and as a Nation.

Ok, what questions do you have for me?