"Delivering AF Cyber Capabilities for the Joint Fight"

Major General Earl D. Matthews
Director, Cyberspace Operations

AFA Air & Space Conference
National Harbor, Maryland
18 September 2012

Major General Matthews: -- policy and guidance necessary to expeditiously move forward into the future.

Since the beginning of our Air Force, air power has been in the DNA of all Airmen. Later we pushed in space. That has been added to our mission statement. Airmen began to culturally appreciate the integration and relevancy of the value of air ad space power together. Today, as you are undoubtedly aware, our Air Force mission has expanded now to include cyber.

This mission is operationally relevant and the capability that it brings to the Air Force is imperative. We must continue to leverage the innovative, imaginative spirit which built our Air Force to becoming the greatest the world has ever known.

We intend to mature and evolve our cyber capability by tapping into the potential of all of our Airmen, being cyber Airmen, to spark the innovation and promise that these men and women have brought to both air and space.

As you can imagine, in General Balsa's first 90 days as the CIO he's had a chance to make a good assessment of where we are and where we need to go. As cyberspace has evolved over the last two decades as we would probably characterize it, the world has focused primarily on net centricity and the Air Force likewise leveraged this collaborative capacity of cyber as a catalyst for other synergistic endeavors.

During that evolution the old com and info community focused on networks, delivering a strong, defense in depth program to defend Air Force networks, anti-virus firewalls and formidable network boundaries, but over time those defensive endeavors gave us a false sense of security. The enemy has developed new tactics and tools to thwart our efforts. New threat vectors have emerged. Like social engineering, spearfishing emails that have attempted and have been successful to solicit information from our Airmen and create more vulnerabilities for the enemy to exploit.

We built this proverbial Maginot Line. Now we have to find ways to defend behind the line, fight through the attacks since our adversary has found ways to be over, under, around and through our defenses. We still need to protect the network, but

we must also protect the reason for the network. The data and information that resides and flows through the network and the value of that information provides must be our focus. For it is to remind us on this information that is at the core of why we do and what we do. In other words, it's time to shift from network focus defensive to more of an information focused defense and about mission assurance.

A good example, maybe a simplistic example, of information focused defense is the steady increase in attention being paid to protecting and securing personally identifiable information or PII. We need to focus on information security, data encryption, stronger policy and procedures to protect our information.

So as one of his first actions as the Chief Information Officer, he published an established a PII policy to limit the transmission of personally identifiable information across Air Force networks and requires encryption any time that it is sent.

As we identify other [inaudible] critical to our Air Force operations we intend to establish similar criteria and policies focused on providing protection of mission essential information and data on our network. To ensure that we can trust the accuracy of our information, especially information like deployment readiness or logistics data. To protect our applications like [Jokes] and Falcon View so that they are available and functioning when we need them. And to determine what is core [inaudible] where we can partner with industry and academia and others to protect our information.

When he took over this position he met with the Secretary and the Chief and he let them know that he intended to use his full authority as the CIO. They both said go for it, Mike, and let us know if you get any headwind. That's exactly what we are doing.

The Chief Information Officer has overall responsibility over a number of cyber-related areas from information resource management, information assurance, and command and control. The CIO is responsible for integrating this information and information-related activities and services across the Air Force and he is the enterprise level strategist and the information and IT architect for our Air Force.

So what does that mean? It means that we are responsible for information for our Air Force. Here are a few things that we're doing from the CIO perspective.

We currently have policies in place that have delivered for years now consolidated small computer buys through AFWAY. We

have enterprise licensing agreements for basic desktop services capabilities with Microsoft. We're now looking into creating IT purchasing efficiencies across our Air Force with Adobe and [Adhoc]. We are partnering with functional communities to deliver enterprise agreements for their systems, namely with Oracle and IBM. There will be others.

We will align our policy with the joint community in every opportunity where it makes sense for the Air Force.

We're also making changes in governance. We have stood up an IT Governance Executive Board. The Board includes three star representation from our acquisition, business transformation, operations, life cycle and [inaudible]. This [inaudible] an enterprise approach for requirements planning, portfolio management and product development across the entire spectrum of Air Force IT to effectively and efficiently how deliver to our customers.

In turn the functional communities who have the responsibility for the lines of operation of our Air Force have now in place a board structure to ensure their systems are integrated across the Air Force enterprise.

The Board will work with the MAJCOMs to help implement policy and enforce governance decisions that we make at the corporate level and that are in the best interests of the Air Force.

That is somewhat General Basla's CIO hat. But he also has the information dominance role that I mentioned.

When he took this job he asked himself the question and he asked the staff the question. What is information dominance? As we thumbed through the doctrine and researched through some of the publications we discovered that in actuality information dominance is not very well defined, so we started to think more about it.

What does information dominance look like for logistics, for ISR, in phase zero or phase four of operations? What does it mean if we don't have information dominance? In thinking about it, information dominance crosses the operational and strategic levels of war, and certainly the tactical level of war. It certainly can affect each of those levels of war and can have the effects at the tactical or operational level of war that cascade them into the strategic level of war. But it also spans all operational phases of a campaign, from shaping to deterring, to enabling civil authorities. Information dominance plays a critical role both in the support and operational areas.

Information dominance affects all mission areas to include but certainly not limited to operations, logistics, joint, special operations, civil authorities. But probably more importantly, it's critical to our national infrastructure and it underpins the current American way of life. Information dominance affects many things that we take for granted in everyday life. Information dominance allows us to apply air, space and cyber power to influence and shape our environment. It is achieved when we have a greater understanding of the strengths and weaknesses and the centers of gravity of an adversary's military, political, economic infrastructure than they have of ours.

Firstly, I see this global in nature and it is certainly the underpinning of the Air Force's global vigilance, global reach and global power.

Information dominance under General Basla's tenure will become the cornerstone of the cyberspace domain. Unfortunately its utility in our business is still misunderstood, a lot like emerging from the air domain was during our historic inter-war periods. If you were one of Billy Mitchell's disciples or understudies at the [Air Force] Tactical School you absolutely knew the criticality and what the importance of the air domain was to warfighting. And you were trying to tell anyone and everyone that would listen how important it was to define the domain and critical to warfighting. Just remember, it's my birthday, I don't want to be brought up on charges. [Laughter].

Now some of the innovative thinking was eventually realized and codified and published in 1943 in Field Manual 100 Tac 20. Command and employment of air power. The first words of FM 100 Tac 20 begins with describing the relationship of our forces and it says, and I quote, "Land power and air power are co-equal and interdependent forces. Neither is an auxiliary of the other."

It's this type of innovative thinking, but it took a long time to become acceptable. But look where it has led our Air Force today.

I think innovative advances in cyber technology will be the game-changer in the next conflict. Make no mistake, it will be the game-changer in the next conflict.

The cyber domain will evolve and dictate changes in tactics, operations and strategy, much the same way that air power technology influenced the outcome of World War II.

Those are our two roles. Chief Information Officer, and Chief Information Dominance Office of the Air Force.

With this in mind, General Basla has developed three priorities which will help us focus our energy. Number one, develop effective IT enterprise solutions. Two, enabling cross-domain resilient cyberspace capabilities. And by cross-domain, make no mistake, across air, space and cyberspace. And third, to foster and grow premier cyberspace Airmen.

On his first priority it seems clear to all of us in this room just by his title, Chief Information Officer, that that's what he's charged with doing. He's charged our team with delivering effective solutions that work for the entire Air Force. That is not to say that we won't pay attention to discreet systems and niche capabilities that are critical to select mission owners. Instead through good policy and smart governance we will maximize our scarce resources to provide effective solutions across the entire enterprise.

We have recently made some strides in enterprise solutions. The Air Force under the leadership of General Shelton and Air Force Space Command has been intentionally migrating to the AFNET over the last few years. This effort works to consolidate Air Force space networks and provide a more secure and standardized data environment. Today we must not focus solely on the more secure, more standardized Air Force network, but also on connecting Air Force networks and information to the joint enterprise.

You may have heard of another initiative that is going on in the department called the Joint Information Enterprise, or JIE. This is an initiative that will take a similar approach to what the services are doing by collapsing networks and data processing centers but more importantly standardize the security architecture amongst the services in the Department of Defense and the internet. This effort will provide better situational awareness and better data protection for systems inside the JIE. But perhaps the most important of those is that these enhancements will greater enable the joint warfighter effectiveness in defending our networks, and just as importantly protecting the information inside as well as leveraging cyber and information to create cross-domain effects.

He intends to keep the inherent air and space core competencies within the Air Force environment, but we will work with our joint partners to migrate to the JIE every place that it makes sense for our Air Force.

As such, the JIE will enable some workload sharing efficiencies across the enterprise such as the Joint Information Enterprise Operation Centers. Those will all be jointly manned.

Now as we transition and we look forward to the JIE there are other capabilities that come to mind. We'll look at improvements such as in identity manning. We can grant access to information based on identities credentials today but not also combined with what role or what job they currently have.

Cloud computing, to enable us to consolidate our current data and services and make it more widely accessible, no matter where you are on the battlefield.

Common security architecture amongst all the services. Again, today we have three or four separate security architectures.

Unified communications, to merge technologies and applications and to reduce our overall infrastructure costs.

So what is the most effective implementation of those technologies for the enterprise? How will we secure them across the enterprise? These are the questions that we are asking and that we need your help, both form industry, academia, those who are operating in the field. Along with the Air Force Space Command who is the core function lead integrator, we look forward to your feedback.

These advancements for the enterprise, both for today and in the future, will help enable cross-domain capabilities. That is our next priority. The enterprise network and services will be the foundation for which we can use information to create effects across those domains. Our capability to leverage information, to create an asymmetric advantage for America is dependent, is absolutely dependent on our ability to maintain freedom to operate in cyberspace.

Equally if not more importantly, is our ability to ensure the confidentiality, the integrity and the availability of our information.

To get information we need resiliency both in hardware and in our applications. Resiliency in cyberspace like resilience in life or on the battlefield is the ability to endure outside stresses from an event, multiple events, and be able to continue or function appropriately.

For example, we need multiple pathways to relay information. If our satellite communication capabilities were to be

temporarily interrupted, how would we pass information to the air crews, warfighters at the edge? We would need an alternate link. Perhaps a radio.

Today we are developing the aerial layer network. In partnership with Air Combat Command and Air Force Space Command and other organizations across the Air Force we are helping to build an aerial network that links our air, space and cyber forces together, providing resilient capabilities in each of those domains.

Now using the aerial layered network our warfighters at the forward edge of the battle will be able to communicate on multiple platforms on the ground, in space, in the air, passing real-time situational awareness with each other in a seamlessly integrated environment. We'll be doing that by deploying smart nodes. These are alternate pathways to communicate should one of these links be interrupted.

Concurrently we're working on a joint aerial layered network. This is to ensure compatibility with our joint partners, coalition partners and to extend our cyber capabilities across that community.

We need to make sure that we have the policies, procedures and guidance that we have established on the aerial layer network to also be the foundation for the joint aerial layer network. Cyber is truly unique because it passes through every single mission area. Nuclear command and control runs on cyber. In fact all command and control runs through cyber. Currently our fifth generation cyber capabilities are 90 percent dependent upon software as compared to the F-4 which was only 5 percent dependent on software. Our highly capable F-22 as well as future tankers and bombers will integrate into and rely upon the cyberspace domain. If you don't know, we can't launch either one of those aircraft -- the F-22 or the F-35 -- without the network being established and operating and secure.

You know what? Up to this point I haven't even mentioned remotely piloted aircraft. We've seen the evolution through the last ten years of RPAs moving from traditional reconnaissance roles to putting bombs on target. The capabilities and effects that the RPAs deliver are one of the most in demand capabilities the Air Force provides to the joint force today. Not a single RPA mission would be possible without a functioning and secure cyber domain. The foundation of these cross-domain capabilities will be the joint information environment. The AON and the JON as I have described. But just like field commanders working to shape the battlefield to their advantage where they can maximize their capabilities, we too are shaping the cyber domain and

delivering asymmetric advantage across all those domains, mission areas, and operational phases of the campaign.

So this leads me to the final and perhaps our first priority. While delivering effective IT solutions are vital to enhancing our cyber capabilities, none, none of it would be possible without growing and fostering the premier cyberspace Airmen to accomplish our mission.

For the core [inaudible] fields, today we give our cyber operators -- officer, enlisted and civilians -- six months of technical operations training. Students receive the highest quality of classified instruction on mobile, space and satellite networks as well as they learn about supervisory control and data acquisition or SCADA. These systems and other industrial [functioning] systems that are used for remote operations of power, dams and so forth. This training gives them a well-rounded understanding and a depth of knowledge regarding cyber networks and systems such that the Air Force would be able to support a homeland defense mission.

Our training provides hands-on experience. It requires performance that is directly related to cyber Airmen in follow-on assignments, much like we do in pilot training. Once our Airmen are fully mission capable we will employ them in a variety of jobs that range across the spectrum of operations as we do today.

Cyber Airmen lead hunter teams on the network in search of terrorists; employ active network defense measures that are engaged with unknown potentially dangerous actors and deploy with the joint special operations forces today and provide support for field work, for cyber forensics.

If you can imagine it, we probably do it.

Furthermore, we have multiple cyberspace continuing education programs. Programs such as Cyber 200 and Cyber 300 at Wright-Patterson Air Force Base. This offers opportunity for our Airmen to continue to sharpen their technical skills, collaborate with other cyber warriors including joint cyber warriors who also attend these courses, and to continue their overall professional education.

Despite our [inaudible] there is now a Cyber Weapons Instructor Course at Nellis Air Force Base. That will keep our Airmen on the cutting edge of cyber operations and technology and the first class graduated in June.

I need to digress here for a minute. That's a big deal. A Cyber Weapons School is very important to us. When you put a

cyber operations officer next to an intelligence officer next to an F-22 pilot and a space operator and they work together now to plan and execute missions, that is real power creating magnified effects on the battlefield.

But probably the greatest benefit of that is that they develop a relationship, a trust, and they figure out that non-kinetic effects are just as valuable as kinetic effects.

These relationships will pay dividends to our Air Force when our pilots and space operators know by name who their cyber operations officer is and know how each will contribute to that mission.

This new training and education comes at a crucial time for our cyber operators. We face challenges in our manpower allocation as our role in cyber operations continues to grow. With our Air Force and joint warfighting growing reliance on cyber I believe we might not have nearly enough of the Airmen we need to accomplish the goals that have been set out for us.

We need to work with the joint community to clearly understand the joint warfighter cyberspace requirements so that we can posture our forces appropriately to contribute to those missions. With this in mind we will partner with our joint brothers and sisters and create a stronger and more interoperable cyber team. We must and we will find innovative [inaudible] in today's resource-constrained environment that will meet the enterprise-wide requirements but also enable our capabilities to enhance our ability to use information to create domain effects and develop advantages over our adversaries.

WE will smartly incorporate our total force brothers and sisters to maximize their diverse capabilities. And we will continue to look to industry for providing cost-effective solutions to growing cyberspace needs.

As we embrace innovation and face challenges in cyber today we will need to consider that all of us are Airmen, cyber Airmen to some degree. Every one of us works, plays, learns, teaches, operates cyber throughout every single work day. By definition that makes us all cyber Airmen.

Just last week I personally watched a pilot use his 3G iPad in the cockpit to check the latest weather forecast and to file his flight plan. While not all of us are charged with operating through cyberspace every day, to enable some type of delivering asymmetric effect, let us not forget that we are all cyber Airmen.

In closing, cyber has brought us a significant shift in our Air Force but no different than the fundamental changes that occurred at the introduction of aircraft over a century ago. But the reality is nobody knows what cyber will look like in ten years or one hundred years.

What we do know is that with the current rate of change it will look vastly different than what it is today.

In the coming years we will be confronted with a growing community of cyber adversaries. We will continue to battle austere extremist terrorist groups as they seek to undermine the freedom that we have in any way they can. So our challenge is to build relationships across the joint community, industry and academia; to build an inclusive team so we cannot fail at any aspect of the cyber mission. We have been entrusted with the responsibility to operate and defend this newest battlefield and deny the adversary the same capability. We've been asked to lead the Air Force and this nation in the cyber arena. How will we respond?

Thank you very much for this opportunity to speak to you. God bless you, Godspeed and help us fly, fight and win in air, space and cyberspace. Thank you.

Question: General Welsh recently said that [inaudible] Congress and the White House [inaudible]. It seems to me that this challenge [inaudible] the mission. So I'm guessing [inaudible]. How do you think that's going to play out?

Major General Matthews: Thank you, Mr. Laducci.

The boss recognized that and when he had his first meeting with the Secretary and the new Chief they talked about conducting a Cyber Summit in the Air Force. So in the middle of November we're going to conduct a Cyber Summit with all the four stars. Because the Secretary recognizes that just because of the evolution and the time period we've been talking about, not all four stars can talk as eloquently about cyber as they can about air and space power. Then here later this week we're actually going to take a lot of our four stars and three stars up to Fort Meade to visit NSA and USCYBERCOM and then we'll get an immersion day preparatory for Air Force discussions and the Cyber Summit.

During the Cyber Summit we will cover the mission that we currently are conducting in the Air Force in regards to the cyber. What should manpower look like, organizationally how should we be organized, and what are the resources that are required to get to whatever level the Air Force deems that

capacity is going to be that we provide to the joint warfighters. So thank you.

Question: How prepared are we to deal with an environment where it's not the traditional [inaudible] or China but an 18 year old kid [inaudible] computer genius that poses a threat to us?

Major General Matthews: I think we're pretty well prepared to address that threat. I think what's most important, as I mentioned, is that we are, under the JIE, that we are taking the current networks and we are architecting them for warfighting so that you would have the resiliency to fight through, even if we [inaudible] capacity of some sort. But I think we're very well prepared to address that.

Question: I just talked to [inaudible] Israeli Air Force and the Australia Air Force about their recruiting plans for cyber warriors. They're both screening 18 year olds very early on, identifying [inaudible] that they really [inaudible]. Now they're looking at the idea of going down into 13 and 14 year olds and catching them even earlier.

Do you have any planning device for how you might screen, identify and train those folks?

Major General Matthews: Thank you for the question. This is my kudos to Air Force Association. They conduct Cyber Patriot which is a big competition every year. There are some other national level, collegiate level and so forth. There's a lot of partnering that's going on now between the winners of these competitions and participants with the local high schools and junior high schools.

But I personally believe we need to have a national education campaign in regards to cyber, much akin to what we did in the 50s in regard to nuclear warfare and we had duck and cover. Now I don't suggest that we have an alarmist view of that, but more like John F. Kennedy did when he challenged the nation to go to space. You see all the great improvements that have happened since the early Corona days in the '60s all the way now to GPS as a mainstay. I think that awareness needs to transcend the entire national fabric.

We are losing the equivalent of the holdings of the library of Congress every year through intrusions from academia, our defense contractors, or the government as a whole.

Question: If the individual hacker, the [inaudible] model is no longer the big threat, you are looking at more those, you

can't say China, at least you can't, but the near peer adversary who's well resourced, especially with that coming in the context of not just [inaudible] but alongside operations as part of a major conflict. How do you move from the perimeter defense, that Maginot Line, the lone hacker, lone guy to this defense in depth, protect the data approach that can fight through, as you say. What different things you can do.

Major General Matthews: One is how the network is actually architected and put together. The diversity of the network. Identifying the critical mission sets that need to be done. Not everything can be protected at the same level. It certainly goes through education and training of our people.

The biggest vulnerability that we still have today with regards to the network is the individual. So everyone has to be cognizant about what they're doing and how they operate [inaudible] on the network.

Question: Going back to the recruiting and looking at '13 and '14 levels, is the Air Force doing anything to look at [inaudible] not so traditional resource?

Major General Matthews: We have in a lot of areas, even serious gaming, a number of our COCOMs and some of our major commands are looking at the gaming community and how [inaudible] live constructive virtual training and so forth. So yes, we are.

Question: Sir, you talk about the intel officer, cyber operator, space operator, pilot and what capabilities that could bring whenever they [work] together. From your office are there any initiatives with regard to policy, training, [inaudible] in linking cyber and space so that you can have that interchange [inaudible] positive [inaudible], more effectively [inaudible] what you call the cross-domain effect?

Major General Matthews: We're still somewhat at the infancy of this discussion. The Air Force created these four functions, these integrators for the 12 core functions of the Air Force. That's only been in existence for about a year now, and so there are still discussions on what should those roles and authorities be for those core function integrators, the biggest emphasis being on the integration piece of it. What is required for us in policy and so forth so that we can make sure that we have the complete generation across all those domains.

Specifically I can address the functional manpower piece of it because I am the functional manager for the 17 Delta community which is the cyberspace operations. We are working very broadly with my counterparts on the intel side and the 13S side. So from

a manpower perspective, how do we start purposely assigning people at a younger part in their career to another domain so that by the time they get to O4 or O5 that they have a broader perspective and they can command one of those units. So we're making pretty good progress on that front.

For those in the audience, the Air Force is leading the way here when we talk about cyber training. My predecessor, Brigadier General Dave Cotton, retired, he's down here on the front row. His team put together the retooling of all our technical training for both officer and enlisted down at Keesler about three years ago. We actually conduct undergraduate cyber training. Recently we took a look at the 42 cyber work rules that have been defined by USCYBERCOM and we matched that up on how we're doing that technical training. We're doing pretty darn good. Then when you marry that up with advanced network warfare training that we also conduct, you'd be very proud on how the Air Force is leading that. None of the other services had that today. Again, at my level on partnering with those other services to see how do we deliver a joint cyber person so that when you're a combatant commander and you do a request for forces and you say I want a cyber guy, that when I get one from the Air Force I know what capabilities he has, but when I also have one from the Navy and the Army I'm getting the same type of person.

Question: You see the cyber domain growing. Do you have a vision in 15 or 20 years where this domain [inaudible] separate service? Space and cyber?

Major General Matthews: Thank you. I wear a space badge and I came in on the early days of the space force. We're just celebrating 30 years of Air Force Space Command being set up. That debate also happened during the '80s, should we have a separate space force. You're the first person I've run into at a public forum that's actually asked me that question. I don't think we need a separate cyber force because the effects of what's happening crosses everybody's domain. So if you start breaking that apart and you have a separate cyber force I don't think you're going to get the synergistic effects that you need to have across all the other domains. I honestly believe that [inaudible] needs to have this capacity and capability. It doesn't belong to just one service.

Question: [Inaudible]? Is there training for officers [inaudible] to increase awareness for [inaudible] the strengths and the problems that we're facing [inaudible]?

Major General Matthews: We've worked hard with all the communities so there's a level of cyber awareness that goes all the way from basic training up to when a person graduates from

basic training and technical training. Then on-line in the Air Force portal we have an IT, EIT learning center that is available to everybody that has all the courses that someone who's in that domain that needs to take it to keep up their level of education, that's available to anybody.

Question: As we know, [inaudible] critical infrastructure vulnerabilities. What's your assessment there? Does the Air Force have any role in helping defend this critical [inaudible]?

Major General Matthews: There are certainly vulnerabilities there from the national perspective. Currently the Air Force is not assigned a role in that regard. But to that end we're, as I mentioned in my remarks, we're teaching the SCADA systems and the infrastructure, how you attach infrastructure, in our undergraduate cyber training so that we can protect Air Force infrastructure that we have on our bases in that same regard.

At the national level there's a lot of synergy and discussion with NSA, USCYBERCOM and Homeland Security who has that responsibility. We're seeing a greater level of information sharing amongst all those agencies.

Question: The Marine Corps [inaudible] program that gives them [inaudible]. EA-6Bs and UAVs and the [inaudible]. Do you envision an expeditionary electronics fire [inaudible] type of program for the Air Force?

Major General Matthews: There was a recent article in I think the Air Force Journal here recently that talked about how you would call for support, cyber support, and the Marines and the Army developed the applications so the person on the battlefield could do it. That was all derived from what the Air Force had created. It was nice to see some publicity about that.

Now if your question is specifically are we going to create some forward units that do that? Or is it about how do you call for those effects on the battlefield?

Question: Yeah. How do you --

Major General Matthews: So silently behind the scenes the Air Forces that created this process and has been adopted is actually being publicized by the other services more so than by the Air Force.

Question: How do you identify it [Inaudible]? Is it a tactical organization?

Major General Matthews: You call for that effect just like you'd call for close air support through the operations center.

Question: Sir, you mentioned the challenge that we have [inaudible] for [inaudible] that's going on. Are there any steps or missions that will allow the Air Force to accelerate on the more traditional acquisition [inaudible]?

Major General Matthews: thank you. There was some NDA language that came out last year, I believe, 2011, that asked the services to take a look at how to do that. The Air Force has internalized that. We have a thing called Fire Starter which is our acquisition piece on how do we get after that. We've stood up an acquisition organization in San Antonio, down by 24th Air Force under the new LCMC in order to foster that.

We're right ta the infancy of that but I see that as a great starter to make that happen.

# # # #