Remarks of the Honorable Michael B. Donley
Secretary of the Air Force
Air Force Association CyberFutures Conference
Gaylord National Resort
Friday, March 23, 2012
(As Prepared for Delivery)

Introduction

Chairman Schlitt, thank you for your kind introduction. Good afternoon, everyone. I want to thank Sandy, Mike Dunn, and the AFA team for hosting this event and inviting me to participate in AFA's second annual CyberFutures Conference. It's good to be with you.

You have heard or will be hearing from a number of Air Force leaders at this conference, including: General William Shelton, Commander of Air Force Space Command, which is the lead for our cyberspace operations; Major General Suzanne Vautrinot, Commander of the 24th Air Force, which supports the cyberspace operations needs of our Combatant Commanders; Air Force Chief Scientist Dr. Mark Maybury; and Lieutenant General Larry James, Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (ISR). So I'm pleased to be part of this impressive lineup for the chance to share my thoughts on the Air Force and cyberspace.

You know, the Air Force has always been a forward leaning military service, always at the forefront applying new technologies to strengthen U.S. national security. And throughout our history, we have demonstrated the flexibility to evolve according to changing needs and requirements.

Our Service predecessors were pioneers who led the way during the early days of aviation, when airpower's potential military applications were first imagined and realized, and our airpower doctrine was being written and tested for the first time.

As decades passed, our airpower theory, strategy, and tactics evolved alongside the development of ever more advanced aircraft and weapon systems. By the mid-20th century, with the emergence of the nuclear age and the dawning the space age, Air Force leaders were again prompted to shift our thinking, to change and develop new strategies to make the most of the national security capabilities provided by the latest state-of-the-art technologies.

With this context, we can better understand that as a collection of technologies and as a domain of operations, cyberspace is just the latest arena offering the Air Force the challenge and the opportunity to keep

evolving as we again wrestle with technology and policy issues right on the cutting edge of national security.

But more than that, we recognize that as cyber-related technologies transform the way we communicate, share information, provide services, and conduct any number of daily tasks, the Air Force cannot afford to stand on the sidelines. Much like the inventors who created the technologies of the 20th century, today's innovators will redefine our expectations and expand our capabilities as cyberspace continues to develop and mature.

And we are determined to ensure that the Air Force is ready to leverage these state-of-the-art technologies, that we have the right plans and strategies in place, and that our cyber operations and cyber support Airmen have the skills and the training they need to meet the defense challenges and opportunities this newest frontier presents.

Cyberspace is an Air Force Priority

As the only domain created by man, cyberspace is dynamic and evolving. Its operations support and closely interact with operations in all of the other domains – land, sea, air, and space. And through the integration of air, space, and cyberspace operations, the Air Force is

developing unique capabilities that support military operations across the spectrum of conflict.

While the term “cyberspace” is most frequently associated with the Internet, for the military, cyberspace encompasses a network of information technologies, including telecommunications networks, computer systems, and embedded processors, as well as wireless logistics systems, land mobile radios, cell phones, integrated air defense systems and satellite systems, and aircraft communication and computer components.

Access to reliable communications and information networks like these makes it possible for today’s modern forces to operate effectively at a high operations tempo. Our military depends on resilient, reliable, and effective cyberspace assets to respond to crises, conduct operations, project power abroad, and keep forces safe.

Therefore, it is no wonder that cyberspace is a priority for the Air Force and the Department of Defense. Last summer, Defense Secretary Leon Panetta put a fine point on it. He called cyber “the battlefield of the future,” and observed that “we are all going to have to work very hard not only to defend against cyber attacks, but to be aggressive with regard to cyber attacks as well.”

To protect America in the 21st century, it is clear that we must further develop and sustain freedom of action in the cyber domain, because even as we increasingly employ these assets, the United States constantly faces the threat of cyber attack and intrusion efforts. Every day, nations, rogue states, criminals, and terrorists seek to infiltrate Defense networks, trying to surreptitiously exfiltrate information, corrupt data, degrade or shut down operations. Consequently, protecting cyber assets and preventing service disruptions are critical national security objectives.

Increasingly, success in warfare depends on the rapid collection, processing, and dissemination of electrons – who collects them or blocks them, who can integrate multiple data sources, and who can decide and execute a course of action. In some cases, as General Keith Alexander has noted, this OODA loop of observing, orienting, deciding, and acting operates at network speed.

Air Force Cyberspace Superiority Budget

To address these challenges, the Air Force is committed to enhancing our capabilities and defending against threats to our cyber assets. This commitment is reflected in the Air Force's recent budget proposal.

While Air Force leaders made many hard decisions to align the FY13 budget request with the new defense strategic guidance and with the cuts required by the Budget Control Act, we made a concerted effort to protect funding for the Air Force's top priorities. And this is good news for Air Force cyber programs, which fared comparatively well in this constrained budget environment.

Our FY13 budget request for cyberspace superiority is $4.0 billion. This funding will support consolidating and improving network security and capability. It will allow the Air Force to continue investing in advanced technologies to monitor and secure both classified and unclassified networks. This includes the ongoing migration toward a Single Air Force Network, which will increase our network situational awareness and improve information sharing and transport capabilities.

We plan to expand our ability to rapidly acquire network defense tools, and develop Joint standardization and acquisition strategies to enable quick delivery of cyber capabilities. For example, upgrades to the Air Force Wideband Enterprise terminals will provide Joint standardization and greater bandwidth.

In addition, the Air Force is working with the Office of the Secretary of Defense to define near and long-term solutions to deliver warfighting communications capabilities by upgrading aircraft and satellite communications systems.

Moreover, we have made considerable progress in our efforts to meet the emerging challenges and threats in cyberspace by fielding a Total Force of over 45,000 trained and certified professionals equipped to ensure continuity of operations in cyberspace. We will build on those efforts this year by establishing three new Total Force cyber units -- two Air National Guard Information Operations Squadrons (IOS), to be located in Washington State and California, and one Air Force Reserve Active Association with the 33rd Network Warfare Squadron (NWS) at Lackland Air Force Base in Texas. We are also expanding the Maryland Air National Guard 175th Network Warfare Squadron.

Developing Air Force Cyber Plans and Strategy

Complementing the initiatives supported by the budget proposal, the Air Force has been taking a close look at our overall strategy, policy, and plans for cyberspace.

We have launched a study, Air Force Cyber Vision 2025, to articulate our near-, mid-, and long-term science and technology strategy. This study – led by the Office of the Chief Scientist in collaboration with our Major Commands, the Air Force Research Laboratory, and the acquisition community – will bring together the best insights from industry, academia, our national laboratories, and other government partners.

Last year, we stood up an Air Force Cyber Integration Group (AF-CIG), to provide oversight and guidance for key cyberspace initiatives. Through the AF-CIG, we're progressing well with our work on a draft Air Force Cyberspace Roadmap. This effort has already identified a series of objectives, based on existing strategies and high-level guidance, to provide a holistic, integrated way forward for Air Force cyberspace.

We also have a Cyberspace Superiority Core Function Master Plan, prepared last year under the auspices of Air Force Space Command. The

Master Plan is designed to help us shape future resourcing so we develop the capabilities needed to support Air Force and Joint Combatant Commanders' desired objectives and effects. Over time, the Master Plan's strategy to reduce legacy defensive structures and processes, which are manpower intensive, will allow the Air Force to recapitalize resources into more flexible and dynamic capabilities.

Another objective of the Master Plan prioritizes the capabilities that will allow us to change the way the Air Force thinks about the cyberspace mission, essentially shifting our mindset on cyberspace. We've often been accustomed to thinking about the majority of cyberspace as a support mission only, but we need to recognize the operational roles of cyberspace operations and support personnel in assuring the Air Force mission, not just protecting the network. This shift in mindset is intended to help Air Force members better understand their contribution to the Joint fight and produce greater operational integration across all domains. The Air Force's strength is Airmen who know how to connect dots for commanders across the air-space-cyber domains.

Cyber Workforce Development

Threats to America in cyberspace are real, and with rapid advances in technology and dynamic security challenges, the Air Force increasingly relies on its cyberspace forces and their ability to anticipate, adapt, and innovate. Ensuring that we take care of our Airmen and that we develop the cyber workforce we need is an enduring responsibility.

For the foreseeable future, we will need Airmen who specialize and excel in Offensive Cyberspace Operations, Defensive Cyberspace Operations, and Cyberspace Support. Our aim is to develop mission-focused cyberspace forces who think and train as warfighters. And we want to make cyberspace an attractive career specialty to those who have the talents we need and those who have the aptitude and motivation to learn.

To that end, we're transforming our workforce, with the stand-up of cyberspace professional career fields, formalization of Undergraduate Cyber Training, maturing mission qualification training for Cyberspace Weapon Systems, and adding more cyber courses, including final validation of a Cyber Weapons Instructor Course.

Although cyber skills recruitment and retention is not a problem at this time, the Air Force is considering programs, such as Selective Reenlistment Bonuses, that may be required to recruit and retain the best talent. It's simply a fact that the Air Force and the government sector at large cannot always compete with the financial incentives available in the private sector to people with cyber experience and expertise.

Nevertheless, there are other incentives that lead people into public service, and we want Airmen and potential Airmen to recognize the exciting cyberspace career opportunities the Air Force offers. Based on Air Force recruiting experience over many decades, we know that the opportunity to be part of a new and growing technical career field, tackling critical cyber challenges, while also serving and protecting our Nation, should provide strong motivation for ambitious and talented young people.

But we should be open to considering other incentives as new generations enter the workforce with expectations that may be different than the expectations of previous generations. Finding the best ways to attract and retain the right talent will always be the key to maintaining a robust and highly capable force, in the cyber field or any other career specialty.

Development of Cyber Requirements and Forces

The growth and development of cyber requirements and forces are still in the formative period and may not exhibit the pattern of growth – such as rapidly increasing manpower and IT budgets – that some might expect. In this formative period, more holistic integration and management of the cyber enterprise is leading to efficiencies in people and in the cost of operations. The savings from these efficiencies are being plowed back into other cyber or related Air Force needs.

But even within our constrained manpower and budget environment, it remains important that our Air Force continue to evolve and reshape itself internally to meet the demands of rapidly changing threats and technologies.

Conclusion

As we consider the future, it's daunting to imagine the changes that may be in store for our Nation. But if the transformative air and space technologies of the 20th century are any guide to where we may be headed with cyberspace in the 21st century, we are in for an exciting adventure.

Cyberspace may be the newest recognized operational domain, but its importance in the way we think, the way we organize, train, and equip

our forces, is becoming more evident all the time. Today's Joint missions in the air, space, and in all domains are increasingly dependent on skilled and innovative cyberspace forces. As such, access and continued freedom of maneuver within cyberspace is an essential requirement for our networked force.

Our proud history shows that the Air Force has successfully developed and adapted new technologies for national security purposes in the past. Our technology-driven force thrives on the kinds of challenges cyberspace presents to today's scientists, innovators, and strategists. As the cyberspace domain rapidly evolves and matures, the Air Force must maintain pace and evolve as well, ensuring we provide ready, reliable, effective, and resilient cyber forces.

We must maintain our commitment to resourcing cyberspace superiority, developing innovative cyber plans and strategies, developing and acquiring the best technology, and, most importantly, building the intellectual capital and expertise of our Airmen who make it all work. Doing so will contribute greatly to our national defense, as well as reinforce our proud position as the world's finest Air Force.

###