Cyberspace as a domain in which the Air Force flies and fights.

Secretary of the Air Force Michael W. Wynne Remarks as delivered to the C41SR Integration Conference, Crystal City, Va., Nov. 2, 2006

I want to discuss with you today a subject I regard as extremely critical: the freedom of Cyberspace.

Just last week Deputy Secretary of Defense Gordon England, speaking before a major network warfare audience, listed the attempts of hackers, "Cyber-vigilantes", terrorists, and even hostile nation-states to degrade our fighting networks as the single issue that he spends "more time thinking about in the middle of the night, than any other."

Before addressing dyberspace directly, I want to set some context, first as to the mission of the Air Force, then as to the topics of this conference, and also as to what we are learning from current combat.

The mission of the Air Force is to deliver sovereign options for the defense of the United States of America and its global interests--to fly and fight in air, space and cyberspace. This was defined a year ago, and then codified a month later, on December 5, 2005.

"Delivering sovereign options" means operating across the Joint spectrum so that we provide to the President scalable choices that are unlimited by distance and time, and span the entire range from humanitarian assistance to nuclear strike, kinetic and non-kinetic.

In Short: Global Reach, Global Vigilance, Global Power.

This includes the powerful option to use timely information to deter and to avoid use of kinetic weaponry. General Curtis LeMay emphasized this when he said, "Peace is our Profession," making it the slogan of the Strategic Air Command.

All these options have one common foundation--persistent, lethal, overwhelming air, space and cyberspace power massed and brought to bear anywhere, anytime.

Thus, the Air Force serves by being prepared to set strategic, and then, if needed, also tactical, conditions for deterrence, dissuasion, or defeat, and in this way offer to our commanders options throughout the spectrum of conflict.

Air Force Chief of Staff General Moseley likes to say, "the soul of an Air Force is range and payload." I would salt and pepper persistence in there as well. That is why after 53 years we are again seeking 21st Century parallel strategic assets in the form of new tankers and global strike to meet our responsibilities in the air domain, emphasizing expeditionary, as well as persistent Strategic options, to ensure the robustness of the nation's global power; and recognizing that the replacement of our satellite constellation is at hand, to fulfill our global vigilance task.

Now, consider how cyberspace stands in relation to the topic of this conference. The topic is "C41SR." For many in the military and certainly for others in the daily walk of life, it helps to take a moment and parse the elements of the acronym.

There are four "C's"--command, control; computers, and communication, then, intelligence, surveillance and reconnaissance.

It started with "command and control", an old military studies term. Nowadays the two words are separated as being two individual items, subject to debate. There was even sometimes confusion as to whether the "I" is "intelligence" or "information."

Here are some things to notice. First, the whole term C41SR has the mantle of familiarity--we don't step back and pick it apart.

Second, each component is a function--not a battle domain, but a function--a form of activity or service.

Third, the six functions are a grab-bag, bundled over the years. While connected in a sense as functions that move data, they are disparate as to physics. But by common assent, we group them for conversation. This facilitates research in the varied areas of sensors, electronic attack, and access and compiling of commander-level Information extracted from gathered data.

Finally, the functions all are vital flows within each of the battle domains of land, sea, air, space, and, as we shall see, in cyberspace.

I have brought a video that illustrates the flows of C41SR functions--that means, the flow of data--in battle, today. As you watch the video I ask you to consider two questions:

First, now that we have enhanced the application space for networked operations; and really moved communications trust and reliability to a prominent position in our concept of operations; how do we defend the net on which all our capabilities depend?

Second, what new habits of thought do we need to adopt in order to create the capacity to deter, guard, rescue, strike, and assess in what will probably be the cyberfight of the 21st century?

The video illustrates the components of what I call the "Information Mosaic"--the whole data net, analog and digital; pixels and composites images; from all sensors that can be collected and downloaded and crossloaded for use by all in the fight.

By filtering critical data from the "Information Mosaic" to the strategic planner and right out to the weapon system itself, we increase flexibility and lethality. This requires common gateways such as cursor on target to maximize data usage. As Assistant Secretary of Defense John Grimes recently put it--it is about the data, and maximizing access.

All the information flow moves in the Cyber Domain, meaning, the entire flow can be vulnerable to a Cyberspace attack.

Let's look at the two questions I asked before the video:

First: How shall we defend the communication net on which all our capabilities depend? This question is critical:

Our ability to fight in ground, sea, air, and space depends on communications that could be

attacked thru cyberspace.

The capital cost of entry into the cyberspace domain is low. The threat is, that a foe can mass forces to weaken the network that supports our operations in any Battle Domain. The other side of the coin of netcentric operations is cybervulnerability

The answer is that defending and fighting in the cyber domain is absolutely critical to maintain operations in ground, sea, air and space.

The second question is: What new habits of thought do we need in order to create and develop technology, and to fight in the 21st century?

The answer is to go back to my comment at the start, and think in terms of trust. Our operations in each of our services all rely on trust.

That is, the pilot can trust information that a target is the foe, not innocent inhabitants of a school building or hospital or embassy.

The groundfighter with a communication device can trust that the device is not being tracked by a foe, potentially exposing the ground force unnecessarily.

This new way of war is data-dependent. So we need to think in terms of trust and securing trust.

So, now let us turn to the Imperatives our country confronts in the cyber domain and the actions which the Air Force is taking.

Here are some scenarios that emphasize the Imperatives:

Right now a terrorist lies on his belly in a dusty ditch. He holds a radio transmitter to detonate an improvised explosive device, to kill Americans as they convoy across a stretch of broken asphalt. His use of cyberspace is currently being contested, but not always.

Right now a drug trafficker sits under a tarp in a boat, bobbing off a Caribbean beach, setting up, potentially, a cocaine drop for nightfall. He gets GPS coordinates on a SATCOM phone from a controller a continent away. His use of cyberspace is practically uncontested.

Right now a finance technician is moving U.S. dollars via laptop to support terrorist ops, while sipping coffee in an internet cafe. His use of cyberspace is practically uncontested.

Right now a foreign government engineer is in the Net using stolen American technology to build radar and navigational jammers to counter American air superiority. His use of cyberspace is uncontested.

Right now a foreign hacker is crashing an American server that holds a web site with data he does not like. His use of cyberspace is uncontested, though subject to pursuit.

Right now rogue securities traders, sex traffickers and data thieves are poised at computers worldwide, reaching into the American net. In a speech just last week, Attorney General Alberto Gonzales voiced his concern about the predators who range through cyberspace, accosting our children. Their access to cyberspace is uncontested, though, again, they are subject to some pursuit.

Each of these examples is real. I could name many more.

What we are seeing is that the cyberspace domain contains the same seeds for criminal, pirate, transnational, and government-sponsored mischief as we have contended with in the domains of land, sea, air, and now contemplate as space continues to mature.

This reminds us of the history that it is military capabilities that long ago helped make it possible to free the Barbary Coast of pirates, so that our world of commerce and ideas could enjoy freedom of the seas, and that freedom of the seas continues to be sustained thanks to the U.S. Navy and Coast Guard partnership with the appropriate authorities in coastal jurisdictions.

This refers also to the idea that America's operations in air and space set the strategic conditions for world commerce to enjoy freedom of the skies.

I am told that by far the larger portion of the goods in commerce worldwide, by value, travel by Air. The remainder moves by sea, mostly bulky commodities. Freedom of the skies is undergirded by the US Air Force, more than by any other power or force, just as freedom of the seas is undergirded by the U.S. Navy and Coast Guard, again in partnership with the right authorities.

In sum, in cyberspace our military, America and indeed all of world commerce face the challenge of modern day pirates, of many stripes and kinds, stealing money, harassing our families, and threatening our ability to fight on ground, air, land and in space.

The National Strategy to Secure Cyberspace states:

"A spectrum of malicious actors can, and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security."

The Strategy calls upon national security planners specifically to:

■ "Improve capabilities for attack attribution and response."

■ "Improve coordination for responding to cyber attacks within the U.S. national security community."

■ "Foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge."

Now, my duty as the Secretary of the Air Force is to put the nation's most technologically capable force on a path to do our share of the task of presenting to our combatant commanders, and so to the President and the nation, the trained and ready forces they may need to ensure the same security and freedom of cyberspace that Americans and indeed many in the world already enjoy in the oceans, in the air, and also in space.

This duty is joint, and, as I have noted, it is interdependent. The duty is to bring to the fight what the Air Force has to offer, and to exercise good stewardship of the Air Force personnel and resources that are in some cases already devoted to operations in cyberspace.

This does not mean "control" of cyberspace, any more than the other domains of ground or maritime. It does mean making our contribution to securing the benefits of cyberspace for our military and, indirectly, for our national and even world commerce.

This means recognizing that the idea of freedom of cyberspace may in time be the same kind of principle as freedom of the seas and freedom of the skies. This means that cyberspace is a domain on which many rely and in which warfighting can, and, actually by some definitions already, takes place.

One rough and ready demonstration that cyberspace is a true domain on a par with land, air, space and sea is to apply the basic questions of the principles of war.

For example, Can one mass forces in cyber? Yes. Does surprise give an advantage in cyber? Of course. Simplicity? Economy of force? Clarity of objective? Yes, Yes, and Yes.

Here is a call for the professional military. The domain is new, but the trained mind of the uniformed warfighter is needed to wage this Fight.

Just as the air domain is governed by aerodynamic forces, and the space domain by orbital mechanics, cyberspace has mathematical, and electromagnetic principles at work. Due to the size of the global information grid and easy access to the electromagnetic spectrum, effects in cyberspace can take place nearly simultaneously at many places. Effects can be massive or precise, lasting or transitory, kinetic or non-kinetic, lethal or non-lethal.

The definition of cyberspace must be broad enough to enable us to integrate the vast possibilities that the electromagnetic spectrum offers now and for the future. Last month, the Joint Chiefs of Staff defined cyberspace as:

"A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."

This definition is being codified in The National Military Strategy for Cyberspace Operations.

Today I am announcing the steps the Air Force is taking towards establishing an Air Force Cyberspace Command.

The aim is to develop ultimately a major command that stands alongside Air Force Space Command and Air Combat Command as the providers of forces on whom the President, combatant commanders and the American people can rely for preserving freedom of access and commerce in air, space, and, now, cyberspace.

Let me summarize the major developments we've undertaken in the past year and the plans for developing the capability to contribute to do our job in ensuring freedom of cyberspace.

In December 2005, General Moseley and I restated the Air Force mission statement to include cyberspace as a domain where the Air Force delivers sovereign options.

This step simply recognized the existing fact that significant Air Force personnel and technology have long been engaged in fighting in cyberspace.

Good stewardship means attending to the systematic training, organizing, and equipping that is

our job. This includes especially attending to the career progression of the Airmen involved in cyberspace, including our Guard, Reserve, and civilian professionals.

The step included consultation with General James Cartwright, the commanding general of U.S. Strategic Command, for he is a principal commander to whom I have the duty to present organized, trained and equipped cyberspace forces.

We stood up a Cyberspace Task Force in January, led by military strategist Doctor Lani Kass. She is with us today. Lani, could you please stand so we can thank you?

The task force, composed of officers from across the Air Force, has spent the past ten months gathering data, researching options.

We addressed cyberspace extensively at the four-star level during a major warfighting meeting in July. General Moseley and I have subsequently tasked the commanders of Air Combat Command and Air Force Space Command to submit a proposal for establishing an operational command for Cyberspace.

We tasked the commander of Air Education and Training Command to develop a training plan and the commander of Materiel Command to analyze the resourcing plans with Air Staff assistance to support an operational cyberspace command.

The new Cyber Command is designated as the 8th Air Force, with a long and strategic deep strike heritage, under the leadership of Lieutenant General Robert Elder. He will develop the force by reaching across all Air Force Commands to draw appropriate leaders and personnel.

The 67th Wing, and other elements under 8th Air Force, provides the center of mass for this startup activity. General Elder remains as a force provider to combatant commanders.

Simultaneously, General Elder has been asked by General Moseley and me to develop a roadmap that could be used to grow the Cyberspace Command "upwards", and has the framework of a full major command, a peer with Air Combat Command and Air Force Space Command. We expect that this work will stretch out for the bulk of this next year.

The mission of bombers now within the 8th Air Force will be remaining.

It is fitting that this historic step, the elevation of cyber to major command status, will take place from the heart of the 8th Air Force. The 8th Air Force is a home of heroes.

In World War II, it was a breakthrough force, bringing a new strategic dimension to the fight. It was the vision of such leaders as Hap Arnold, Ira Eaker and Curtis LeMay. In this century, the Eighth Air Force will be the home of new breakthroughs. This is a noble home for the mission of ensuring freedom in a whole new domain.

As I close, here are key points to bear in mind:

■ The focus is to make the Air Force mission complete from an organize, train, and equip basis. Properly presenting trained and ready forces offers the right sovereign options in this domain.

■ This is a battle domain in which the Air Force operates with, and supports our sister services, first responders, and many times non-government organizations and the many non-military

authorities who also work to keep cyberspace secure. There are many partners across this domain.

■ There will be careers and a strong future for the Airmen whose work is in the cyberspace domain. Air Force personnel experts are at work now forming the career and schooling paths that ensure a full career with full opportunities for advancement to the highest ranks of the Air Force, for our military and civilian professionals.

■ When planning and fighting in cyberspace as a battle domain, the task is one for the professional warfighter, that is, the trained military professional who lives, and breathes, and thinks the principles of war. The Air Force has long had these professionals in uniform, and I honor them for their service to our country.

As I look across this room, I marvel at the harnessing of technology, the invention of applications, and the representation of the strength that each of you embody.

It gives me confidence that freedom of cyberspace will be secured. The technological innovations that many of you are directly responsible for, plus the courage and bravery of our networked force, from missile defense to tactical commanders, and the men and women they command, defend every day the freedoms we enjoy in all five domains.

And now, I turn to you and conclude with this question. I hope that each of you can ponder it and help our services and our country find the best answers:

"In this 21st Century, how shall we best carry out the C4ISR functions in the cyberspace domain?"

Thank you for your service, for your continued support; and may God continue to bless the United States of America. Thanks for allowing me the honor to provide the keynote address for this important forum.