

Cyberspace: A Warfighting Domain

Dr. Lani Kass
Special Assistant to the Chief of Staff

26 September 2007

Moderator: Good morning. On behalf of the Air Force Association it is my honor this session to introduce our speaker.

She's a special person. She is the Special Assistant to the Chief of Staff of the Air Force. She is leading the Cyberspace Task Force. She is a senior mentor to Checkmate, and I can assure you that they are not planning attacks on Iran. She is a former professor at the National War College, and as such when I was at National Defense University she worked for me, or maybe it was vice versa. I'm not sure I know. She's the author of two books and over 20 articles and I'd like everybody to join me in welcoming Dr. Lani Kass.

[Applause].

Dr. Kass: Good morning.

Some of you have heard General Elder speak very eloquently last night about his efforts as the Commander of the 8th Air Force, soon to be the Cyber Command. If I was setting the agenda I would probably set the briefings in the reverse order because I'm going to provide you the conceptual foundation that has led our Air Force to claim another domain. And based on that, General Elder and now General [Billy Lode], the commander of the provisional command, are working to implement this vision.

What I want to do is take you on a journey of an intellectual discovery and there were moments as we were working this, and what you'll see is really the product of an effort which lasted about a year.

Any one of you who has worked in a bureaucracy knows how difficult it is to do something fairly massive in the course of a year. We are there because we need to be.

Next slide, please.

We need to be there for two related reasons. One, a blinding flash of the obvious. The United States is at war. The United States is at war with an enemy who threatens us not just kinetically, but an enemy who is using modern means of communication to spread a message, to spread an ideology, to recruit, to collect money, to fund and finance an organization whose desired end state is world domination. It is as simple and as politically incorrect as it gets.

So picture modern communication means in the hands of Nazi Germany or Communist Russia. So we are at war. Our enemies, declared enemies who have declared war on the United States, Western civilization and modern Arab regimes, are using the cyber domain to mobilize, recruit and promulgate their message. So this is the fight we are in, the fight we might be in in the future --

Next slide please.

-- is with opponents, potential components and peer competitors who have discovered that there is a fifth warfighting domain. I will talk at length, at least as the time allows, about this fifth domain, the electromagnetic spectrum. Limited physics, since I slept through most of it in high school, but you need to understand what it is.

Let me put the bottom line up front as you listen to this presentation. Perhaps for the first time in the history of warfare, there is a domain that allows you to deliver effects disproportionate to the level of investment. Let me repeat that. To dominate on land, at sea, in the air, and in space, you need to invest a fairly significant amount of capital, training, equipment, and continue to evolve that equipment to stay ahead or at least level with your competition.

In the electromagnetic spectrum of the cyber domain a very minimal investment allows you to inflict damage totally disproportionate to your level of investment.

Next slide please.

You can see growing recognition in the national guidance of the United States, growing recognition of what is at stake and what is being threatened.

I will point to you two interesting things. It took two years since September 11 for the national strategy to recognize that there is a need to secure cyberspace. At the time, in 2003, the focus was on critical information systems. As you continue to today and the binding document is the 2006 National Military Strategy for Cyberspace Operations, a document which is classified, signed in a fairly unusual manner by both the Secretary of Defense and the Chairman of the Joint Chiefs, for the first time ever the definition of cyberspace as a warfighting domain, a domain which like air, favors the offense.

I had an opportunity to talk to a young Air Force officer on the first day of this conference who told me no one has come up with a good definition of cyberspace. So I'm here to tell you, this is a pretty good definition of cyberspace. It is the domain of electronics and electromagnetic spectrum. It is a warfighting

domain. And it is a warfighting domain because our enemies made it so.

Next slide please.

To keep it short I am not going to show you the evolution of the Air Force's mission and intent over the years tracking, paralleling the evolution of the National Security Strategy. Let me just point to key inflection points.

The first one being December 7, 2005, coincidentally or in great recognition for history, Pearl Harbor Day. The new mission for the United States was proclaimed, including for the very first time since the establishment of an independent Air Force a new domain - cyberspace.

In his congressional testimony a year later our Chief stated very clearly what it is that we're going to do to accomplish that mission. We are going to treat cyber as a warfighting domain and we're going to establish a Cyber Command co-equal to, alongside with, Space Command and Air Combat Command. Okay? At the same testimony General Moseley also defined cyberspace in probably the most compelling manner. From DC to daylight, direct current to daylight, to radio waves, microwaves, gamma rays and rays we have never even thought about. That's pretty good. It's good enough for me.

Next slide.

This is difficult. A lot of people say we're cutting force structure, we cut 40,000 people. How in God's name are we going to support and finance a whole new domain?

The point I'm making is we have been there before. Less than a decade into powered flight visionaries and pioneers were seeing the military potential of aviation. And yes, they were people who were saying they're a bunch of geeks who probably just couldn't make it in the cavalry and therefore you're trying to use this new invention of the Wright Brothers as an instrument of war.

Next slide.

But pretty quickly it became recognized as a warfighting domain and not just a warfighting domain in the sense that you can deliver effects in it, but as a warfighting domain allowing you a new concept - cross-domain dominance. When Billy Mitchell at the Battle of San Miguel uses air power to affect conditions on the ground; when he bombs the captured German ship [Ospreland], demonstrating you can affect events on the sea from the air, air power becomes more than just a curiosity. It becomes a new warfighting domain.

You know what happens to Billy Mitchell? Not too many people listened to him in the euphoria of the Roaring '20s.

Next slide.

Consequently the notion of cross-domain dominance conceived by Billy Mitchell gets implemented in wartime not by the United States and the Western allies; it gets implemented in the devastating combination of cross-domain effects of land and air and sea called the Blitzkrieg. This is Billy Mitchell's notion taken to its logical extension.

As you know, the enemy decided how this war is going to start. The Western allies determined how this war is going to end in the Battle of Britain over Dresden, Schweinfurt, and [Ploeste], and ultimately over Hiroshima and Nagasaki.

But air power as the lynch pin of cross-domain dominance, is born in the crucibles of World War I and World War II.

Next slide.

Over the next decade air power has expanded into new domains and new frontiers. And here is another point that I would like you to take away, that low globe, with the little [inaudible] that you see in the right hand corner on the slide, that wasn't ours. That's the Sputnik. There is a built-in assumption in all our analysis, in all our planning, that the next military invention of significant military impact is going to happen in the West. It is an assumption. And like many assumptions, it might be proven in the crucible of war to be the wrong assumption.

But the point I'm trying to make here is innovation, evolution, revolutionary thinking are second nature to Airmen.

Next slide please.

But while we have a culture of innovation and adaptability, if you think about it, air power evolved over three parallel tracks. You had air, you had space, and you had enabling operations along the electromagnetic spectrum.

By the '90s, by the mid '90s, the three domains did not fuse but were added together to produce better effect. In other words, air power was supported by space power was supported by information technology. Consequently in Desert Storm for the first time you saw a new application of air power as a sum of air, space, and the electromagnetic spectrum.

Next slide.

We are now merging into a new warfighting domain. We call it cyber. I presume to call it the electromagnetic spectrum. You can call it whatever you want. If it senses, connects, controls, signals, transmits and processes, it is operating in the electromagnetic spectrum and it can produce a spectrum of effects. The physical properties of the domain, the electromagnetic spectrum, allows you to modulate those effects just like air or sea or space or land. Submarines don't fly too well. Tanks don't float. Electronics operate along the electromagnetic spectrum and if it is a warfighting domain, like in any domain you need to control it. You need to assure that you have freedom from attack, but you also have freedom to attack.

Next slide.

I keep talking about the electromagnetic spectrum. To all of you who, like me, slept through high school physics, this is just a reminder. This is what the electromagnetic spectrum is. Okay? So anybody who equates cyber with computers, note if you please where the focus is. There is an old IBM computer in a wooden box. Here you have the Victorian internet, the telegraph; followed by the radio, by the mobile phone and the PC. Everybody that talks about cyberspace as if it was exclusively computers misses the point.

Two points to remember from high school physics. The further to the right you go on the electromagnetic spectrum the higher the velocity of energy. The energy moves faster and it's greater. And the further to the right you move on the electromagnetic spectrum the higher the scale of effect you can deliver. Hence the notion from DC to daylight, from gamma rays to rays we have not even thought about before,

We have been in that domain before. I used the term the Victorian internet. The telegraph came into being during the American Civil War. There in the corner is Billy Mitchell stringing wire in Alaska. Right next to him is the World War II Air Operation Center during the Battle of Britain.

My point is, we have been using the electromagnetic spectrum longer than we have been using air and space. What we have not done yet and we are on the path to do is integrate, fuse, these three domains.

Next slide, please.

Remember the mission said fly and fight in air, space and cyberspace.

Remember how I said at the beginning for the first time in the history of warfare we are dealing with a domain where the

level of investment is disproportionate to the kind of effects you can deliver.

The point I'm trying to make is if you don't dominate cyber, you cannot dominate in air or in space. You cannot dominate on the land and at sea. Quite frankly, if you're a developed country, you cannot conduct your daily way of life. Your life essentially comes to a screeching halt.

When you're dealing with something new, we all apply what we know. When the Chief said okay, what does it mean to fly and fight in cyber? My first thought was well, how different would it be from the concepts that have led us to fly and fight in the air and in space and for that matter on land and at sea over the centuries?

Cyber favors the offense. If you're defending, you are late. Defense in cyberspace in my humble opinion is a loser's game. Cyber allows you to deliver on the original promise of air power to win wars quickly, with less human suffering, and with less damage. If you can deter, dissuade, deny or defeat without resorting to TNT, think about the range of possibilities this opens.

If you can deliver global effects at the speed of light, not just at the speed of sound; if you can bring your opponent to a screeching halt without blowing anything up, you miss the visually pleasing destruction but you achieve effects that don't look too good on CNN, or don't look at all on CNN, and you don't need to spend billions of dollars to rebuild the kinetic damage that you have caused.

Next slide.

You will hear the Chief in a few hours talk about redefining air power for the 21st Century. This is a piece, a facet I the mosaic. This is a piece of bringing air power to the 21st Century by creating a synergy of effects, not air plus space plus cyberspace, but rather a synergy multiplying the effects you can deliver in the air, through and in space, and through and in cyberspace, and you can do it from the global to the theater level, from the strategic to the operational level, truly fulfilling air power's mission.

Next slide.

So this is where we are. This is what I am talking about. For the first time ever we are on the threshold of integrating the full spectrum of effects not only in the three domains that I talked about before - air, space, and cyberspace - but also on land and at sea. Allowing us or whoever masters that the ability

to deliver effects globally any time, any place at the speed of sound or the speed of light.

Next slide.

This is the other facet in the revolution that the Chief is going to be talking to you about. This is 21st Century global reach, global power, global vigilance. The term we have coined is cross domain dominance.

Back to Billy Mitchell. Back to demonstrating that you can effect from one domain to another. Except this takes more than air, land and sea. It integrates air supremacy with space supremacy and cyber supremacy to truly redefine warfare. And as you will see from the slide, and I don't want to dwell about it too much because those operations are being fleshed out as we speak, the operations that you conduct, the type of operations that you conduct in cyber to achieve cyber supremacy are not that different from operations you conduct in the air to attain air supremacy. You still do combat and you still do mobility except along the electromagnetic spectrum both the combat and the mobility transmit energy at the speed of light. You still need a similar set of capabilities, capabilities for strategic attack, directly into the opponent's centers of gravity. You need a counter-air capability or counter-cyber capability. You need the ability to do interdiction. You need the ability to transmit information. And you need to provide close cyber support. Again, those concepts are being fleshed out as we speak. This is a revolutionary idea.

Next slide.

Why are we doing it? The reason we are doing it is because the United States Air Force is our nation's premier cross-dimensional maneuver force. It is also the sword and shield for not only our nation but the global alliance.

So the notion here of revolutionizing air power for the 21st Century is the ability to use the inherent attributes of air power to deliver effects precisely, quickly, persistently, at the speed of sound and at the speed of light.

In the American way of war where we fight jointly, if you do not control air, space and cyberspace, quite frankly it doesn't matter how big your Army is and it doesn't matter how many ships your Navy has. The first battle of any future war is going to be for control of air, space and cyberspace. And frankly, if you want to pulse within that, the first battle is going to be for control of cyber.

Next slide please.

This is what we are doing. There are a whole bunch of what the Chief lovingly calls [trolls and nons] who have issues wrapping themselves around a revolutionary concept and the inherent question is what's in, what's out?

The Secretary asked me one day a very valid question. How many people in the United States Air Force are doing cyber. I said everybody. No, no. Really doing cyber for a living, operating across the electromagnetic spectrum, using that spectrum to deliver effects. The answer is 40,000 people of the total force. That's quite a few people. Do we need a command to provide an umbrella for 40,000 people? Yeah, I would say so.

Somebody asked General Elder yesterday, where are we going to find the people and the resources? The people are there. The resources are invested. But we're using them as a utility. So here is a point for you to think about. When you flip the light switch or you flush the water in the toilet, how many times do you think about the brave men and women that deliver your water and electricity? We have learned to take this for granted.

The point is our enemies understand how important it is, how this is the Achilles hell of every modern military, and how the first battle is going to be to control this.

So we are approaching it holistically, we are developing a comprehensive enterprise starting with what it is that we need to deliver effects in this domain. We need a set of enabling capabilities, supporting and sustaining capabilities, and again, those things exist. They need to be put together and organized properly, kind of like an independent Air Force.

This will be my last slide.

This is really important and I will end on this slide. Huge mission for the Guard and Reserve. I'm really happy that general Bradley, who has been a huge supporter of this effort, General McKinley is not here, unfortunately, huge mission for the Guard and the Reserve. Think about it. People are doing that on a daily basis and we are planning to develop cyber warriors not as a bunch of geeks. I want a bunch of trained killers who understand that non-kinetic does not mean non-lethal. Let me repeat that because most people confuse the terms. Non-kinetic, meaning there is no boom, no big explosion, does not mean non-lethal. So this is a warfighting domain in which you need experts on how to deliver these kinds of effects. You need operational planners and weapons officers just like you need in air and space. And you need strategic leaders and planners and programmers who are going to take both the Air Force and the joint community into this new domain.

Okay, roll the movie.

[Movie shown - transcript follows].

Our condolences and our prayers go out to the victims, families and their friends.

An F-117 based at Holloman Air Force Base in New Mexico went down during a raid over Kosovo. The pilot, operating out of Aviano Air Base in Italy suffered only minor scratches and was picked up.

Back in New York at 10:29 the North Tower of the World Trade Center collapses.

In the past the enemy has exploited the use of cyberspace to their benefit. Cyberspace is the electromagnetic spectrum from DC to daylight, to gamma rays and beyond.

In cyberspace we sense, signal, connect, transmit, process, and control to deliver both destructive and non-destructive effects.

The United States Air Force recognizes cyberspace as a warfighting domain equal to that of land, air, sea and space. Future military success will require the mastery of this domain.

The initial concept of cyberspace was developed in the 1940s by Norbert Wiener, the Father of Cybernetics. Wiener's application of the science was simple. Cybernetics is communication and control, or in other words, it allows us to affect processes through communication and feedback to achieve near real-time predictability to deliver effects.

The control of cyberspace is critical to our ability to observe, orient, decide and act against the enemy. We call this the [uda] loop. Within this [uda] loop we must integrate sensors, achieve predictive situational awareness, exercise dynamic command and control, and finally deliver the necessary kinetic and non-kinetic effects on the enemy.

Let's consider how this theoretical concept might play out in a real world scenario on a tactical level.

A parameter defense [falinx] operator team takes mortar fire from an enemy position. The operators act quickly and successfully neutralize the enemy's fire. But instead of responding by striking this enemy position with counter-battery fire, they relay the insurgents' counter-battery coordinates to an airborne sensor/shooter platform. The airborne platform quickly finds, tracks, fixes and fires on the enemy's position, killing or wounding several of them. As the enemy contingent evacuates the area the airborne platform tracks their movement.

Based on the track of the insurgent movement the operators anticipate that they are heading for medical treatment. The airborne platform operator passes this essential information to a friendly ground team which intercepts the insurgents as they arrive at the medical facility. The insurgents are taken into custody for questioning and intelligence gathering. Critical intelligence reveals the location of insurgent leadership and active operational command and control - a key target in eliminating insurgent influence across the region.

Many nations are embracing cyberspace both in action and in doctrine. Future conflicts could be decided by who masters this domain first.

Successful operational control of cyberspace will enhance our freedom of action while simultaneously denying the enemy's freedom of action across the electromagnetic spectrum.

The Air Force is activating combat-ready forces trained and equipped to conduct sustained combat operations throughout the electromagnetic spectrum to fully integrate air, space and cyberspace operations in the joint battlespace.

[End movie].

Dr. Kass: At least the English is better than mine. Any questions?

Question: Dr. Kass, in 1997 the President's Commission reported out and the Commission was led by retired Air Force General Marsh, and he pointed out vulnerabilities in our critical infrastructure - in the banking system, the power grids, the cell phones, et cetera. Here we are a decade later, we have no legal definition of what an attack, how it's defined, how it's constituted.

In addition we've gotten notifications of an ongoing level of attack activity on the Naval War College, universities, the Pentagon and many businesses.

So my question very simply to you is A, are we a little late to need here? And B, have we bitten off more than we can chew?

Dr. Kass: Let me take the second first. We don't have a choice. You pretty much summed it up.

I conducted a very small public opinion poll among my friends which demonstrates one of two things. Either I need a better set of friends, or this is true. I asked a very simple question. Who do you think protects your sovereign right to shop on Amazon.com? The answer among all my friends was the military, of course. Well the answer is not really. That is by national

guidance the responsibility of the Department of Homeland Security. Now if you liked Katrina that will give you a lot of confidence. Okay?

So my two nightmare scenarios are one, an electronic Pearl Harbor, meaning a deliberate, devastating attack by our enemies on something that the United States probably more than any other country relies on in its daily activities. We literally could not conduct our way of life if we could not use the electromagnetic spectrum for everything that we do.

But my second scenario is a Katrina scenario. Now Katrina was a naturally-occurring event. But what happened in Katrina was that the civil structures whose responsibility it was to take care of what was happening, collapsed. More accurately, the scale of the disaster exceeded their ability to deal with it. Then who are you going to call?

Well, in Katrina the military was called, of course. The military is neither resourced nor equipped nor authorized by law to protect the civilian infrastructure.

I will tell you in my humble opinion in the cyber domain, technology has far out-paced policy, legislation, international law.

When Estonia was attacked in the cyber domain not very long ago, bringing the government of a sovereign country to a screeching halt, NATO sent computer engineers. Now if Estonia was attacked from the air would we invoke Article 5, attack on one is attack on all?

So the point I want you to ponder is, the technology is there whether we like it or not. Our ability to deal with it, you're exactly right, has been lagging tremendously. Today it is much easier to get permission to kill the enemy, to drop a bomb on a terrorist hideout, than to culturally offend them. In other words, take a beheading video, take it off the net, and substitute, or whatever you like, Bay Watch. The technology is there. It's there in the civilian world. But the policies are such that you can't do that.

So yeah, I would absolutely agree. Legislation, policies and international law are lagging the technology and yes, the United States is late to the fight.

Question: Not a question but a statement, if you don't mind. A couple of sentences.

We actually did not just begin this rodeo. In 1999 the Secretary of Defense directed that an organization be set up and a joint task force was set up to provide computer network

defense. It was called JTFCND. An Air Force general, Soup Campbell, was the first commander of that. So their job was to, with these couple of hundred people, look after all DoD computer networks. That was their responsibility.

A couple of years later a computer network attack planning function was added to that organization and it was called JTFCFNO, computer network operations. That operation continued for a couple of years and then was developed into a global network operations JTF which earlier had belonged, those functions had belonged under U.S. Space Command. When that went away those functions were transferred to U.S. Strategic Command who now owns JTF global network operations.

Dr. Kass: Actually both.

Question: And the authorities to do some of the things that you're talking about, of course, still a lot of that in development. But we've been working on this for a long time in the Department of Defense. I think this is a very timely standup of an important command. But we were concerned about this for a number of years and have been doing something about it. Perhaps not enough, but at least there is some history there of computer network defense operations and attack planning help for combatant commanders.

Dr. Kass: Thank you.

Moderator: We've got the next speaker in line. Let me suggest that we put Dr. Kass down in the right corner over here and you can all approach her with personal questions.

I do want to thank Dr. Kass for her insightful presentation and I'm sorry we ran out of time on this one. It's a lesson learned for us for the future.

#