

What I would like to do for the next several minutes is offer you a short glimpse of what we see from a totally unclassified point of view, what China is doing in cyberspace. We've had the opportunity over the past couple of years to look at this issue and write quite extensively on it, so we'll proceed here.

Actually, we've written three books. The one on the left was written in 2004, *Dragon Bites*. The one on the right, *Decoding the Virtual Dragon*, was written in 2007. And the one in the middle, *The Dragon's Quantum Leap* is coming out, I think, Friday. These books are not available on Amazon, they're government printing press books. So if you want them, you really need to write us, they're free. I've seen both *Dragon Bites* and *Decoding* on Amazon going for \$180. Please don't pay that kind of money, they're free. They advertise them as extremely rare. That's because somebody who got a free book sold it to them and that's the way it goes.

What we've covered in these books, though, I believe, gives you a real good overview of the theory and practice of what China is doing. And the Chinese Economic Commission just produced a report that was really equally good in giving you this overview, especially the last ten pages, I thought, where they gave a case study of how one company has tried to meet the challenge of what really was a massive Chinese reconnaissance and exfiltration exercise where they actually had breach teams and collection teams and their reconnaissance effort probably occurred over two or three years in order to obtain passwords and everything else that was required. So, you'll really get a good look at just the depth of their penetration and how focused they are on exfiltrating either intelligence information or conducting economic espionage.

When we traveled to China, we have the opportunity on occasion to pick up books. This is one I picked up in November, *Internet Wars*, and I offer it to you because it offers you some of the thinking when you look at just the chapter titles, I'm not going to go beyond that, but of 18 chapter titles as you see here. The inevitable internet war, the internet will determine victory in future war, financial wars in the internet world. There is a great

focus in that country because they take an entirely different view of strategy than we do. In this country, we focus on ends, ways and means, that's our strategic mantra, it seems. However, over there they look strategically, holistically, big picture. They look at the objective environment, we look at the operational environment. They're two entirely different things when you're looking at things from a Chinese perspective. I think that's why you really see their focus on politics and economics a little more integrated into the military sphere across the board.

We were looking not long ago at this book, a Chinese book, called *China's Revolution in Military Affairs*. And this particularly quote kind of jumps out at you, that "war with the objective of expanding territory has basically withdrawn from the stage of history. Even war with the objective of fighting for natural resources is now giving way to this idea of controlling the flow of financial capital." And certainly, U.S. companies, U.S. banks have seen this in the past couple years.

When the Chinese look at cyberspace, I feel that they look at it from a very different perspective than we do. And I'd offer you these three ways to consider. Historically when you think of something like Sun's *Art of War*, when you think of something like *Make Noise in the West, Attack in the East*, we seldom in this country think in terms of using packets of electrons to do that. They do. We've actually used very similar concepts; for example in Iraq in '91, rustle the grass to startle the snake, an old stratagem. We were able to see where the radars were. We had the Iraqis turn them on, obviously, by giving them some false decoys. We rustled the grass to startle the snake. They do the same thing with packets of electrons and it's just something we need to be aware of. It's a totally different way of looking at the problem.

Secondly, they have this concept called comprehensive national power. Comprehensive national power, again, gives you a very different strategic overview. They're looking at the entire objective world. And when you say objective world, what we mean is the Chinese are looking at objective factors. What's the level of science and technology in the United States? Where are our troops located? How much of the GDP is spent on

defense? Then you find a way subjectively to manipulate those factors. That is the essence of strategy, which is very different from ends, ways and means.

Finally, this idea of laws and regulations are different than ours, ask Google. If you've been following the press the past couple of days, you found that financial industrial Google, several countries have been hit by what certainly appears to be Chinese espionage. And today in the paper, Google delayed the launch of two phones in China. But the interesting thing was the comment from the Chinese foreign industry, to me, which said this, "Foreign enterprises in China need to adhere to China's laws and regulations." You can't make this stuff up. This is the way they look at the world, it's their laws, their regulations. They're very different than ours. In fact, for those of you who've read the Chinese book on restricted war, one of those methods that they had was to look for vulnerabilities, ways to manipulate international law to their benefit. And certainly, it seems that through cyberspace, they found a way to do that.

Some of you might ask what is a stratagem? I almost feel like it's an effects-based operation. We have that term, but as you see here, the stratagem is designed to mislead enemy processes of perception, thinking, emotion and will. Very similar in all ways, I think, to an effects-based operation. What effect are you trying to achieve?

Another point that you might be interested in when looking at China is how they control their own people. They have these little characters that every 30 minutes march across your screen to remind you that someone's watching. So they have their own ways of looking at the world and controlling the processes within China itself.

If I was looking at their internet strategy and I wanted to say, "Okay, what could I offer you today?" it might be something along these five points, and I'll show you each one of them here in order. Seeking preemption, we find a lot of writing in China about network warfare deterrence. But as this quote notes, the last sentence, "we should make unremitting efforts to seek such a preemptive opportunity through developing network

technology and systems,” and as you'll see in a few minutes, they talk quite often about system sabotage, warfare, system attack warfare and other such concepts.

Computer reconnaissance, a prerequisite for victory. General Dai was the head of the information operations department of the General Staff in China, and he retired a few years ago. But this book he wrote on direct information warfare, as you see, he talks about computer network reconnaissance being the prerequisite for seizing victory in war. This is something that you read over and over and over again as you pour through Chinese military writings.

The other thing that they want to do during this reconnaissance effort, collect technical parameters and specific properties of all categories of information weapons. So there's this huge intelligence collection effort as well. We've written about it in the office. This particular article's in *Military Review*, China's electronic long-range reconnaissance, so things are there if you're ever interested.

Chinese stratagems and electronic shur (?); again, there's a connection between reconnaissance and stratagems. You have to realize this history of military thinking influences, I think, to a larger degree than we want to believe, a lot of the things they do. A victorious army first wins and then seeks battle. A defeated army first battles and then seeks victory. And reconnaissance enables you to spot those vulnerabilities. It enables you to first win before you seek battle.

Electronic shur, it's chapter 5 of Sun's *Art of War*, and it is seeking to attain a strategic advantage, which is really what a stratagem is trying to do. How do I attain a strategic advantage in peacetime before some other conflict arises? I think most of you know about the reconnaissance of banks, industry, the military, they're still collecting technical parameters. As the report today said about Google, they're doing economic espionage, intelligence collection. There's just a whole series of things that they're out to collect.

an opportunity for response at the end. So let's begin with a few questions from the audience, and who would like to be the first questioner? Yes, please? Please identify yourself and wait for the microphone.

AUDIENCE: Sir, I'm John Shaud, Air University. Like to ask specifically Bob Kehler a question. The chief mentioned as one of the approaches of the 21st century, the whole of government. And you used a remarkable analogy talking about the wonderful world of cyber with that football field to even include the fans. And my question to General Kehler, as you approach this with a whole of government view, sir, how are we doing marching down that road?

DR. PFALTZGRAFF: Hold that question, and now let's get a few more. Who would like to be next? Please, the microphone will come around to you right there. Can you pass it across?

AUDIENCE: Hi, Wing Commander Andy Challen from the British Embassy for General Kehler and also Mr. Thomas. We know that the east and the Chinese and the Asians have got a very patient attitude and we've heard about the long-term reconnaissance that they take part in, and we know that the feudal system hands down the history through the generations. In the west, we are dealt a blow to that by the political agendas and the timings of how we do things. And we've heard today with the speed of reaction of space and cyberspace, how do we mitigate those factors?

DR. PFALTZGRAFF: Okay, who would like to go next? Over here, we have a question?

AUDIENCE: Brian Green with Systems Planning and Analysis, a question for General Kehler. General Schwartz talked about the need to make space systems more responsive, and I wondered if you could give us your current thinking on how to make those systems more responsive, and for whom you would make those more responsive?

DR. PFALTZGRAFF: Okay, thank you. One or two more, we have time? Please, over here?

AUDIENCE: Mr. Hermann, could you tell us what size warhead the commission looked at? The traditional view has been that only megaton class warheads can create the kind of EMP field that would be catastrophic for the U.S. economy. So could you look at that? And for Bob Joseph, what are the lasting contributions of the Bush Administration to counterproliferation, particularly the PSI?

DR. PFALTZGRAFF: Okay, one or two more? Who else would like to go? Is there one more question? Yes?

AUDIENCE: Ted McFarland from Booz Allen. This is for General Kehler. I'd like to hear your views on how industry can help with this-- you talked about cyber acquisition and the need for speed and how we can help close that gap.

DR. PFALTZGRAFF: Okay, well then let's take those questions. By the way, even though they're directed at a particular member of the panel, or members, others I hope will feel free to help to respond. So let's begin, and maybe General Kehler, since you had so many questions directed to you?

GENERAL KEHLER: Yeah, I hope these are panel responses as well. It's been so long I talked, I forgot what I said.

DR. PFALTZGRAFF: The audience hasn't forgotten what you said. [laughter]

GENERAL KEHLER: Okay, let me start with cyber, General Shaud, and your question about whole of government. No question about this, this is a whole of government issue. I think you all hear that. You certainly look at that in the articles that are being written and the discussions that are being held. Here's what we have focused on to date. The

Air Force has come through a very interesting set of discussions about where we wanted to go regarding cyberspace. We made some decisions, the Chief and Secretary made some decisions a year ago at Corona about assigning lead command responsibility to Air Force Space Command, standing up 24th Air Force, going to the AF ISR Agency and having them establish a group that's going to be in direct support of 24th Air Force, giving Dick Weber, the commander of 24th Air Force command authority over the entire Air Force network, et cetera.

If you listen to all of this, this is really about getting the Air Force's house in order regarding cyberspace and starting there. I think we have done that. And here's what we've recognized in the fairly brief time that we have now been consolidating these cyber activities in this command as lead command. What we understand is that there are many lanes regarding cyberspace and that we are in one of them. We recognize that we are not alone, really, even in the lane that we are in. Our Service colleagues are in there with us. We recognize that we are part of a Department of Defense activity that is still emerging and shaping. And we recognize, I believe, as I listen very carefully to the combatant commanders, both General Kevin Chilton, who you'll hear from at a later point in the conversation who has responsibility, unified command plan responsibility for these activities today. And as they are working their way through what the Secretary of Defense has directed us to do as a department and standing up U.S. Cyber Command, we recognize that this is a much bigger issue than the Department of Defense.

And so at this point, our focus is really, sir, on making sure that we are looking at ourselves with two major pieces; actually, three. One is doing a better job in installing the wherewithal to protect ourselves and make sure that we can assure the missions. The second is to make sure that we are able to respond to what the joint war fighters are going to need in terms of Air Force participation and how we will present forces, how we will establish those command relations and all of those mechanical things that are necessary for us to take Air Force capability to the joint team.

And then finally, what we do regarding people and how we prepare ourselves to compete, if you will, for the talent. And you heard the chief mention something about that earlier today. That will be a very interesting piece of how we will go forward. And so we are looking at some alternatives, actually, to take back to the Chief and Secretary on how we will do better on that part in terms of organizing ourselves and training and preparing our people.

We do know this is a bigger picture than us, we can tell you. And Dick Weber, who was here, could tell you that our initial activities, we are in fact supporting STRATCOM today with their activities. As I say, General Chilton is responsible for these activities today within the department. And so we know from their experiences and our component experiences with them that this is clearly a whole of government activity. In some cases, my football field analogy suggests to me that we will not be the major player in cyber and that gets back to it depends on what happens on the football field. You know, if somebody comes in and spray paints something over a player's helmet, that's not an Air Force problem. It's somebody else's problem. If somebody hits somebody and there are civilians who happen to be passing by, that's not the football referee's problem. So this is going to be a very interesting set of authorities, responsibilities, and recognizing that we must be very mindful of protecting Constitutional rights.

DR. PFALTZGRAFF: Let's go across the panel and continue with Bob. Would you like to respond to some questions?

DR. JOSEPH: I wouldn't want to try to respond to any of the technical questions. My background in physics is just two courses deep, physics 101 and physics 101. [laughter] So let me just comment on PSI, on the proliferation security initiative. This was one of the principle tools, new tools, that the Bush Administration did put in place relatively early, I think it was May 2003. And it's one of a number of tools. The others were the globalization of cooperative threat reduction, Nunn-Lugar type programs through g8 funding, United Nations Security Council 1540, which this administration has also pushed forward.

The global initiative to combat nuclear terrorism, which is an initiative that President Bush and President Putin sponsored together, as they did with yet another initiative on managing the growth of nuclear energy in a way that hopefully will be more proliferation resistant. But these tools, and other tools like them, including in the defense area, such as missile defense, and new concepts for deterrence, have to be seen I think in the broader strategic context. And specifically in the three tier strategy that the Bush Administration put forward. And as far as I can tell, is still being implemented, at least in part by the Obama Administration.

PSI specifically has now grown to 95 countries. As most of you know, it's aimed at stopping the trade in proliferation. It has created, I believe, a more proactive sort of stance for the international community to deal with the disruption of the trade in proliferation. And it has had a number of key successes, many of them are classified given the nature of the work that has been done through various intelligence channels. But one that does stand out is the interdiction of the BBC China in October of 2003, which did lead to the unraveling of the A. Q. Khan network as well as to the Libyan decision to abandon its nuclear, chemical and long-range missile programs.

DR. PFALTZGRAFF: Thanks, Bob. General Kehler has a comment or two more to make on questions. So let's go back to general Kehler.

GENERAL KEHLER: I didn't want to ignore the other two questions that came my way. So before we go down the rest of the panel, the question that was asked about the Chinese and sort of how we view them; just let me offer one thought about this. Remember, those of us who have children, remember when you would take the kids to the doctor for their shots when they were little? The doctor always had a blue bear. They would hold up the blue bear like this, and the kid would look and then you'd get the shot? I'm not so sure that the direct ascent ASAT isn't the blue bear. I think we need to be mindful of what the other panelists have said here about philosophy and strategic patience and strategic intent and the other things that go with that.

And so what we need to be careful of, it doesn't matter who we're talking about here, is we need to make sure, I think, that strategically we do not find ourselves in some kind of strategy that imposes things on us, that imposes costs, that imposes those kinds of difficulties on us without being certain or at least fairly certain, that we are on the right strategic path. Which gets to my point about mission assurance here. This isn't about trying to launch the equivalent of the *U.S.S. New Jersey* to orbit, which would take a lot of lift, by the way. I'd use Dr. Joseph's two physics 101 classes and tell you that that's a lot of lift that would be required.

And the second thing, someone asked about responsiveness and how we're thinking about space and space responsiveness. I believe that a responsive space capability that as strategic command has outlined to us, has tiers associated with it-- not t-e-a-r-s, t-i-e-r-s-- tiers that would start with the things that we already have and making those more operationally responsive and goes through a series of steps that allows us to have a national strategic capability to augment or replenish or reconstitute some amount of our capability in concert with a mission assurance approach, which means that we would be looking also at air and cyber for part of that, or maybe a significant part, of that reconstitution depending on the scenario we find ourselves in.

I believe that kind of a responsive space contribution would contribute to deterrence. And that's what our objective ought to be as we go down that road. And I believe today, we have a number of elements that would need to come together to have that. We need to have responsive launch vehicles, we need to have a common command and control system so that we don't redo a command and control every time we put up a small, cheap satellite. We need to have common buses, et cetera, with standards. There are some great things going on, and I know Curt Bedke, (Major General, Commander of Air Force Research Labs) is here, the Air Force Research Lab, and elsewhere, about plug-and-play kinds of things. And then what we need are militarily useful sensors that could plug into them. So those pieces are in work at varying levels. I would tell you, I think we've got three of those four, pretty substantially in work today. We don't like what it

costs, but I think in terms of a crawl/walk/run approach for national security and a strategic capability for us to contribute to deterrence, I think a responsive space capability is necessary.

DR. PFALTZGRAFF: Thank you. Bob?

DR. JOSEPH: Let me just follow up on the China ASAT. It happened, I believe it was early January of 2007, it happened on a Friday during the weekend. The State Department undertook a number of steps to coordinate the response with allies. On Monday, we called in the Chinese ambassador. I had the opportunity to do that. The Chinese ambassador sat there and responded, A, that he didn't know anything about an anti-satellite test; and B, Chinese opposed U.S. weaponization in space. Needless to say, I did have some fun in that meeting in responding.

But what we did afterwards, I think, was even more instructive. And that is we made the rounds to Congress, to argue that this is a major wakeup call and we need to change the way we approach space and particularly our vulnerabilities in space. As far as I can tell, no one's answered that wakeup call. I hope I'm wrong, but I don't believe I am.

DR. PFALTZGRAFF: Thank you. Dr. Hermann, would you like to talk about the mega tonnage issue?

DR. HERMANN: Megatons, right. I can assure you that the commission spent a lot of time on that subject, and there's a couple of elements of what is technically required. And the discussion and the material and the information in those sessions were classified. And so, I can't quite, but let me say as a layman what I think I can tell you.

That both we and the Russians know how to design bombs that will create high electric fields, E&P fields with other than megatons total output. They will create the electric component. It probably takes a big bomb to create a truly disastrous magnetic E3 component.

The next question is, well, would any minor player with a handful of weapons or one or something, would they be able to have it? And then there is a contest between the intelligence community which says we see no evidence. And then there's Rumsfeld who says the absence of evidence is not the evidence of absence. And so there's a discussion as to whether somebody would have the ability to create it. But on the other hand, stealing apparently is a behavior of humans. And so stealing ones that are already developed by somebody seemed to be a possibility. So there is a question about whether or not the cheap shot by a minor player will be fulfilled by some other than a-- it won't be confined to a super power issue. And I would say I came away persuaded that I don't know what people have, but I see a plausible way for somebody to destroy my country unless we actually take modest measures to keep it from being a catastrophe.

DR. PFALTZGRAFF: Timothy Thomas?

MR. THOMAS: With regard to the question about China, I would say they already have a whole of government approach. They really do look at this whole issue holistically. There's an old saying, quantity has a quality all its own. And when you've got about 350 million Chinese who speak English, you have lots of people that they mobilize for cyberspace issues. They also have information industrial exercises over there, they have mobilization exercises quite often. So they really are practicing now in peacetime for something which doesn't sound all that good, to be quite honest with you.

Terminology seems to be to me the one bugaboo that we have in this country. We are so focused on our sound bites and we live by our sound bites and we expect others to live by our sound bites. And I think that's just one of the biggest mistakes we make. For example, take the term asymmetric warfare, I challenge anybody in this room to come up with a Chinese definition of it. They don't think like we do. Asymmetric warfare, one of the definitions I saw was the application of abnormal logic through the exercise of 12 crafty tactics. Now, that's something that we don't even come up with in this country.

And if you don't understand where they're coming from, what strategy is, how they look at these terms, you really are off base from the beginning.

General Schwartz's comment this morning about we need space control, really is something that strikes at the heart of China. They look at control as more important than dominance. They would refer to something like Kosovo and say, "You had information dominance, but you still didn't have information control because the Serbs were able to influence you by some of the things they did on the ground and cause you to shoot weapons at mock-ups and those sort of things." Control is a huge issue for them and it lies at the heart of what they're doing, I think, in many different arenas.

The last thing I'd like to say is just the fact that with the football analogy, I like it. I like this whole idea of being on the playing field. The only thing I worry about is are we scouting the other team? Do we really know what the other team's doing? And if these rules and regulations are not the same, are they playing rugby when we play soccer? Or as General Kehler said, are they the ones who are going to spray paint your face because that's part of their rules and regulations? You really have to think hard about these analogies because it isn't the same team. And if we don't scout them, if we don't know what kind of offense and defense we're playing and we know what we're doing, so what? We got to know what they're doing, too. So, thank you.

DR. PFALTZGRAFF: Dick, you have the last word?

DR. SCHULTZ: Well, I would note that the concept, whole of government, really grows out of the wars that we've actually been fighting since 2001, not ones that we might have to contemplate in the future. And that concept deals with the kind of security environment that I outlined. In Iraq, in Afghanistan and elsewhere, what we found is that we needed a different approach to conflict and security. We learned it the hard way in Iraq, but we learned it.

Now, what that means is that military forces and an array of other capabilities, or military forces doing things that other agencies of the government ought to be doing, have to come to play in order to stabilize the situation and deal with the kinds of conditions that we've been dealing with in the wars we've been fighting. How well are we doing in terms of developing this whole of government approach really is the second part of this project that I mentioned to you.

We're doing okay. To use a football analogy, since it seems prevalent here today and since I played that game for seven years, we've advanced the ball a bit, but we have a long way to go in terms of dealing with the irregular warfare. Now, remember the QDR in 2006 said this regular warfare environment was increasingly what we were going to be involved in. Secretary Gates last year said it's as important, irregular warfare, as the other kinds of warfare we may contemplate fighting in the future. But in terms of a whole of government approach, we're not there yet.

DR. PFALTZGRAFF: I would like on our collective behalf to thank this outstanding panel for its outstanding contribution in helping us to set the stage for what is to follow in this conference. I realized that we are running a few minutes behind schedule, so therefore I hope that you will make the break very brief. Certainly at the maximum, 15 minutes. We will run, of course, a little bit into the lunch hour with the next panel, which promises to be another outstanding contribution to this conference. So again, we adjourn the panel at this time and welcome the new panel in a few minutes.

END OF SESSION I