

AIR, SPACE, AND CYBERSPACE POWER IN THE 21ST CENTURY
38th IFPA-Fletcher Conference on National Security Strategy and Policy

January 20 – 21, 2010

DAY ONE

LUNCHEON ADDRESS

THE HONORABLE MICHAEL NACHT

ROBERT L. PFALTZGRAFF, JR.: Ladies and gentlemen, if I could have your attention while you complete lunch and dessert is served, I would like to introduce our luncheon speaker at this time, and to give him maximum opportunity to interact with you during the time that we have available.

Our speaker is Dr. Michael Nacht, who is Assistant Secretary of Defense for Global Affairs. And, he is someone whom I have known for many, many years, perhaps longer than either he or I like to admit, because we were exchanging some very good academic war stories, so to speak, of the 1980s, which gives you some idea about how long we may have known each other, and maybe even earlier.

Before joining the Obama administration, he served in a number of previous capacities. For example, he served in the Clinton administration as Assistant Director of Strategic and Eurasian Affairs in the Arms Control and Disarmament Agency. And, he was previously a part of NASA. He was, before joining the administration today, the present administration, he was professor of public policy at the University of California in Berkeley and Dean of the Goldman School of Public Policy.

His prior academic affiliations include Dean and professor, School of Public Affairs at the University of Maryland. And, before that, associate professor of public policy and Associate Director at the Center for Science and International Affairs at the Kennedy School at Harvard University.

I might add that Dr. Nacht was a founder and co-editor of the very important and prestigious *Journal International Security* that so many of us, I'm sure, in this room are familiar with. He holds a bachelor of science in aeronautics and astronautics, and a master of science in operations research from New York University, and a master of science and statistics from Case Western Reserve University, and an MA in political science from the New School for Social Research, and, last but not least, a PhD in political science from Columbia University. So, our speaker is, indeed, well educated. So Michael, it is a great pleasure to welcome you as our luncheon speaker today.

[applause]

MICHAEL NACHT: Thank you Bob.

First, let me thank General Schwartz and the U.S. Air Force, Director Ken Meyers and the Defense Reduction Agency, Bob Pfaltzgraff, President of the Institute for Foreign Policy Analysis, and the International Securities Studies Program at the Fletcher School, which I used to know very well, for their hospitality, for putting on this great conference, and for really getting very senior people from the Air Force and other services and other distinguished guests, to come to grips with these very challenging subjects.

I also bring greetings from my colleague Jim Miller, Principle Deputy Under Secretary of Defense for Policy, who regrettably couldn't be with us today.

Let me try and spend, in about 20 minutes, a kind of tour for you of some of the thinking in OSD policy, surrounding some of these reviews that we are conducting and about to complete. We're conducting them with the benefit of many, many other important

stakeholders, which I'll describe in a minute. And then reflect a little bit on what I'm calling "cross-domain deterrence," or "deterrence across domains," as one of the themes.

The more you dive into these subjects, the more you realize we really do live in a complicated world. We have a proliferation of potential adversaries and of potential allies. We have a proliferation of tools of conflict and domains in which conflict are being conducted.

The studies, four of which are mandated by the Congress, is an effort to address how we are going to meet these challenges. The Quadrennial Defense Review and the Ballistic Missile Defense Review are very near completion now. And, the Secretary of Defense, Robert Gates, will be presenting them with the Department of Defense budget February 1st. The Nuclear Posture Review and the Space Posture Review are delayed somewhat. And, there's also an internal cyber strategy analysis that's being done, which will not be made public and is not mandated by the Congress.

In every one of these studies, we have had the benefit of very senior input from the services, from the combatant commanders, from the Joint Staff, from military and civilian leadership throughout the Department of Defense, from selected members of Congress and their staffs, from the White House, from the State Department, in some cases from the Department of Energy, of course the intelligence community, in some cases the Department of Homeland Security, from some representatives of think tanks and the scholarly community, and from other governments. So, I would be misleading you if I didn't say these were highly participatory exercises, involving scores and scores of meetings, briefings, analyses, and exchanges of views.

I mentioned that what we are seeking to do is to offer a set of integrated themes that cut across these studies and issue areas. We know, of course, that we're engaged in two wars: in Afghanistan and Iraq, in which we must prevail because winning matters. Winning matters not only in those conflicts, but winning establishes credibility. Winning

strengthens deterrence. Winning promotes reassurance. And, winning makes the prevention of future conflict more likely.

We are challenged in a couple of the cases, particularly the space and cyber areas, by the fact that increasingly, these are domains that we are calling congested, contested, and competitive.

They're congested because there are just more players. A lot more things happening, a lot more objects in space. And, of course, many, many more players in cyber. They are contested because there are seemingly some adversarial relationships evolving or that could evolve in space and in cyber. And, they're competitive because there is a struggle for technological achievement, for human resource advantage, and other aspects. These are very demanding fields. And, the very best talent is being allocated by governments, by subnational terrorist organizations, by criminal groups, to these areas.

Now, let me just say a word about some of the reviews. I won't say anything further about the QDR or the BMDR, but I'm happy to discuss that in the Q and A period if you'd like. Let me say a word about the Nuclear Posture Review. President Obama has made it a high priority directive to us to find ways to reduce the reliance on nuclear weapons in U.S. national security policy.

It doesn't mean to get rid of them right now. But it does mean to reduce their roles. At the same time, we are directed to strengthen deterrence against adversaries and assurance of allies. And, simultaneously, to maintain a secure, safe, and effective deterrent. So, we have the job of squaring that difficult circle.

A key aim, of course, of the Nuclear Posture Review is to set out a series of ideas and principles and initiatives which can help us deal with what most see now as the dominant nuclear threat, which is not a full exchange of nuclear weapons by states, but rather the nuclear proliferation problem to third countries, the possibility of nuclear weapon use in a regional conflict, the possibility of nuclear weapon use by one of these

states against our allies or against us on the homeland of the United States, and the possibility of nuclear terrorism.

We've found, in some of our discussions with other governments, they don't seem to have quite as high a concern about nuclear terrorism as the U.S. government does. Some governments do, but some do not. But, we feel, very much, that this is a top priority. We have evidence of intent, and we have some evidence of desires to acquire the necessary means to use nuclear weapons by terrorists against our allies, against our forces abroad, and against our homeland.

So, we are establishing a set of pillars that will guide the Nuclear Posture Review. I can't go into much detail now because these are still to be approved by the Secretary of Defense and also reviewed by the President when the Secretary of Defense presents the NPR draft to the President. But, I can say that many of these issues about declaratory policy, about force structure, about infrastructure, about the stockpile, and a number of other areas have been discussed at very high levels in the White House, but we've not yet engaged with the President.

We want to make sure that the document that is produced, which has been called a foundational document of this administration, is well understood by potential adversaries and by our allies. We don't have the slightest intent to weaken our alliance relationships. Just the opposite. And, we must make sure that, as we reduce reliance on nuclear weapons for their security, we demonstrate credibly that, with combinations of more intensive partnering, with missile defense, with conventional global strike capabilities and other means, that we are strengthening deterrence and extended deterrence and assurance, not weakening them.

In the Space Posture Review, we face a complex situation, in organizational terms, because there are two parallel space studies underway. There is a national space policy review that's being conducted by the White House. And, this cuts across all agencies that have space assets, including NASA, the Department of Commerce, and a number

of agencies that don't have a national security mission, as well as the Department of Defense, the intelligence community, and the State Department.

And, while their work is not yet complete, they will produce a national space policy for the nation. In the meantime, we are working with the Director of National Intelligence and his colleagues on a Space Posture Review, which deals with the role of space for national security purposes. And, a follow-on report called the National Security Space Strategy.

Let me say a word about space. We have a wide variety of missions that we conduct in space in the national security area: intelligence, surveillance and reconnaissance; space situational awareness; satellite communication; satellite space protection, and many others: environmental monitoring, for example. There are, perhaps, a dozen identifiable key mission areas.

We are examining each of these to determine what policies, if any, need to be sustained from previous administrations and what need to be altered. If space is becoming a more congested, contested and competitive environment, do we need to change our declaratory policy about space? Do we need to foster more cooperation with other governments? What are the risks of fostering cooperation with other governments? What about with commercial firms? There's a wide variety of commercial actors in space. Which ones can we partner with? Which ones should we not partner with?

And, what happens if there is use of force in space? What is the appropriate U.S. response? How can we deter use of force in space? What do we say about it before it happens? What do we say about it after it happens? This is clearly a growing area of national importance.

And, of course, our space assets are intimately tied to our nuclear forces and to our ballistic missile defense forces and to a variety of other conventional forces. So, this is

where you see the linkages between space assets and the QDR and the NPR. Again, no answers today, but soon.

Let me spend the balance of my time on cyber. A number of us have been taken by the importance and the global coverage of the Google potential departure from China. Where are we with cyber policy? Well, let me begin with a brief summary of something that's happened in the past. You know, as Bob said, I began my life as an engineer, so I'm kind of ultimately more practical. I like to see the stuff fly rather than just look at simulations and PowerPoints and chalk on a blackboard.

Some of you who follow cyber security know that there was a study done by an organization called the U.S. Cyber Consequence Unit. Any of you familiar with that organization? You can get this off the web (<http://www.usccu.us/>).

They did a report on what happened in the Russian cyber attack on Georgia in the summer of 2008. And, they offered five major conclusions. This gives you a little flavor for just the beginning of what we're confronting. First, the cyber attacks against Georgian targets were carried out by civilians with little or no direction from the Russian military.

But then, they go on to say, the organizers of the cyber attacks had advance notice of Russian military operations and were tipped off while the kinetic attacks were being carried out. So, they may not have been connected, but they were well informed.

Social networks operating over the Internet were the main tool used to recruit those carrying out the attacks.

A fourth conclusion: the civilian cyber attackers were aided and supported by Russian organized crime elements.

And fifth, the total number of civilian cyber attackers was much greater than the campaign against Estonia a year or so earlier. But, the total number of computers involved was much smaller.

So, this gives you a little bit of a feel, if you didn't have it before, for the complex interconnections between individuals, criminal groups, and the government, and the tremendous challenge of attribution in cyber attacks and cyber warfare. We are, deeply concerned about this. Our entire society, our entire military force structure is dependent on cyber capability and is, therefore, vulnerable to cyber attack, or could be vulnerable to cyber attack.

What do we do about this? And, what can we do about deterring such attacks? Let me cite, from a personal perspective, a series of possible responses or possible actions we could take before such an attack. We could threaten, directly, credibly, to damage the attacker, assuming we know who the attacker is. We could threaten associates or networks connected to the attacker.

We could increase our defenses to deter, if not dissuade, the potential attacker that they could really cause mischief. We could offer additional exploitation and let the adversaries know, or the potential adversaries know, that we know what they're up to. We can kind of alert them that we're onto their game as a means of deterrence.

We could more ostentatiously build up capabilities to retaliate without doing anything. We could respond to cyber attacks in domains other than cyber, cross-domain attack. We could respond in space. We could respond in the air. We could respond at sea. We could respond on the ground. We could respond economically.

We could formulate, in advance, explicit declaratory policies about cyber, about cyber attack, about criminal cyber behavior, and even articulate what constitutes a cyber action against us that justifies use of force by the United States, which is a complex legal and policy question.

We could raise these issues directly with another government. We could meet with their leadership, or we could meet at intermediate levels and discuss these issues. We could seek bilateral agreements to limit or to stop such actions.

We could move multilaterally, to try to foster international cooperative agreements, or— if not formal treaties—modes of conduct or other norms. We can advise and help our allies, to reassure them that they, themselves, will be assisted by the United States should they be the victim of an attack. We could use existing national security organizations like, of course, our NATO Alliance, to enhance their alliance cyber capabilities.

We're not doing a lot of these things now, but we're considering many of them. Many of us believe we are in the infancy of the cyber warfare era. And, cyber warfare is too threatening to our vital national interests and capabilities to be silent or to think passively about it.

After all, not only are our strategic forces, our flow of conventional forces, dependent on cyber capabilities, but our society, our air traffic controllers, our financial networks, our electric power grids. There are very few key elements of our society that are not potentially vulnerable to cyber attack.

We have found that some adversaries or potential adversaries are exploring but not yet malicious in their actions. They are exploiting information. They are finding out information that we have. Others are exfiltrating. They're taking data we have, acquiring it for their own use, and then acting upon that information. There are some who are planting malicious software in systems of ours, but not activating them, with the prospect that, at some point, they could activate them. And, if they activate the malware, they could cause the systems to malfunction.

If you just let your mind explore this a little bit, I would say this has the potential to be transformational. It could really change the way we think about a lot of things, including

ROBERT L. PFALTZGRAFF, JR.: Well, thank you very much, Michael, for this outstanding contribution. We now have a few minutes, I believe, for questions. And, would you like to field the questions yourself?

MICHAEL NACHT: Why don't you do it.

ROBERT L. PFALTZGRAFF, JR.: You'd rather have me offend people? Okay. Alright. Who would like to begin? In the back here. Please identify yourself.

Q: Don Loren with the Torrey Group. Thank you, Mr. Secretary, for your remarks today. And, thank you for coming back into government. You painted a very formidable picture with your with respect to cyber security. And, could you give us any insight as to where the Department might be going and thinking about, with respect to roles across the entire government, other than just forced protection and mission assurance, how do you see the Department of Defense interacting with the rest whole government approach?

MICHAEL NACHT: That's a great question. First let me say that Deputy Secretary Lynn will be here tomorrow. And I think he's going to address the cyber issue in some detail. So, I don't want to, in any way, encroach on his territory. But, for those of you who follow this, you probably know that the Secretary of Defense announced, back in June, the establishment of Cyber Command, which is a sub-unified command under STRATCOM.

Its initial operating capability has been delayed. The President nominated General Keith Alexander, the Director of the National Security Agency, to be the first combatant commander of Cyber Command. And, we're awaiting his confirmation. Once he is confirmed, Cyber Command will stand up. This will be an effort to integrate the exploitation capability, to some degree, but the defense capability and, if necessary, dynamic-- what we're calling dynamic defense to protect the information networks of the Department of Defense.

The Cyber Command's sole explicit mission is to defend DOD networks, the dot-mil networks. Of course, we have a vast number of Dot-Gov. networks and, beyond that, a huge number of Dot-Com networks. That's not the business of CYBERCOM. CYBERCOM may be asked to contribute, but they won't have the lead.

And, this gets you into the question about whole of government approach, where the Department of Homeland Security will have the dominant role in protecting the dot-gov networks and will clearly rely on capabilities from other agencies to carry out that mission.

Because of sensitivities about civil liberties and privacy issues, there are many delicate legal questions involved in carrying out the cyber mission. It's not just, you know, potentially retaliating against some malicious foreign government's actions, which probably wouldn't necessarily involve complex legal analysis.

You could have an Al Qaeda group in Afghanistan. Afghanistan is an area of hostility. And, we are clearly legally authorized to attack their capabilities in Afghanistan. But Al Qaeda may have a cyber capability that they're utilizing in Central America somewhere. It's not crystal clear the legal conditions that need to be satisfied for the United States to take action against those, what we're sometimes calling neutral space.

So, actions taken in the United States and actions taken in neutral space pose a challenge for us, both in terms of organizational authority, and in terms of legal framework. Actions taken in areas of hostility are pretty clear. There is also a distinction between so-called Title 10 and Title 50 responsibilities, the military actions versus the intelligence actions.

But, you have touched on a very important area. It's taken us a while, and will take us longer to get our, sort of, brains around this. Now that the President has announced Howard Schmidt as the new cyber coordinator in the White House, he will be convening senior level across agency meetings to try to thrash out some of these problems.

ROBERT L. PFALTZGRAFF, JR.: Who would like to ask the next question? Do we have one from over here, for example?

Q: Michael, you said you might have to say something more about the NPR in the question and answer session. We had some discussion earlier in the deterrence panel on prompt growth and response, non-nuclear strategic terms. Could you talk about how that's shaking out? And then, what is the state of the U.S. and Russia negotiations ...(inaudible)?

MICHAEL NACHT: Okay. Well, let me start with the second one. Then I'll go back to the first one. On START, we're now calling that the New Start Treaty, NST, instead of START Follow-On. You know, these negotiations have been going on since April of 2009. They have been very intense.

The first analysis of the Nuclear Posture Review was done was to determine the levels of operationally deployed strategic nuclear weapons and strategic nuclear delivery vehicles that the United States needed to have in order to carry out the current guidance of employment of the force. And, that information was provided to our negotiators. And, that was the guideline for the first set of negotiations, which led, in July 2009, to the agreement by President Obama and President Medvedev to announce these ranges for subsequent agreement, 1,500 to 1,675 operationally deployed strategic nuclear weapons, 500 to 1,100 strategic nuclear delivery vehicles.

Since the fall, there have been intensive negotiations that went on almost every single day, from mid-September through mid-December. You know, we had every hope to complete a treaty before the START Treaty expired on December 5th, or at least by the end of the calendar year. And, we were not successful. I think it's actually been publicly announced that a very high level team has just left for Moscow today to reengage.

So, that's where we are on that. And, we're trying hard. Both President Obama and President Medvedev have said they want the treaty. So, I don't think it's lack of will by the Presidents or by some of their senior staff. We're getting there, but we're not there yet. Possibly next month, possibly in February.

By the way, there will be some technical annexes with the treaty, which might take even longer to work out, even if the treaty language itself is agreed to. So, that might take a few more weeks or months. There are different views about that. So, that's the current status.

On prompt global strike, we have capabilities in these areas that could provide important enhancement of our overall military strength. I think for some, it's seen more as a niche capability to fill certain very specific missions. For others, it has broader applicability. I think you may see something in our report or in other statements that we are not seeking to threaten the Russian nuclear deterrent. We're not trying to do that with conventional forces.

The same thing is true with our ballistic missile defense deployments. If we want strategic stability with Russia, which we do, and if we want to move way beyond nuclear arms control as a basis for the relationship, to talk about all the other things we haven't discussed-- terrorism, energy, and so many other issues, and if we want to do something similar with the Chinese, we can't be in the business of threatening their nuclear deterrent. So, we don't plan to do that.

But, that doesn't mean the strategic rocket forces or the second artillery don't feel we are threatening them. And, in fact, they have told us that they do feel we are. So, we have to find ways to move forward with systems that we think are in our national security, and still allay their concerns that we're really going after them in a very kind of aggressive way. That's a demanding task.

With respect to China, all we can do is try to convey to them our views at multiple levels, which we are doing. And, we're going to see more of that in the next year, I think, engaging with the Chinese at very high levels.

ROBERT L. PFALTZGRAFF, JR.: Michael, I want to thank you for taking the time to be with us today, and for giving us this outstanding *tour de reason* of the many issues that you are dealing with, and which, of course, are of direct relevance to the United States Air Force and to this conference. So, many thanks for being with us.

MICHAEL NACHT: Thank you.

[applause]

END OF SESSION