

**39th IFPA-Fletcher Conference on National Security Strategy and Policy:
The Marine Corps: America's Expeditionary Force in Readiness**

April 14 – 15, 2011

**Dr. Richard H. Shultz, Jr., Professor, and Director, International Security Studies Program, The Fletcher School, Tufts University
Panelist, Session 1, "The 21st-Century Security Setting: Identifying the Demand"**

Questions and Answers

DR. ROBERT L. PFALTZGRAFF, JR.: Well, there's an amazing amount of insight and information here as a result of what we've just heard. And we have, at most, a half-hour, that's not too bad, for discussion. And what I would like to say at the outset is as you ask your question, make sure that you wait for the microphone; it will be coming up to you. You should identify yourself and then speak loudly into the microphone and direct it to any member of the panel.

So who would like to go first? Yes, would you take the microphone back?

R. CORBY THIN[?]: Good morning, my name is R. Corby Thin. This question is directed to Professor Shultz. In COIN operations, you mentioned the success we had in Al Anbar. And I think much of that success was due to the fact that, first, Al Qaeda overplayed their hand. And what they did then is they aroused the interest of the people, and ultimately we empowered the people to protect themselves. In our mission in Afghanistan, we seem to be working a different strategy, where instead of empowering the people bottom up, what we're attempting to do is to empower a government that is largely regarded as both removed and corrupt, and to a certain degree, consequently, disempowering the people at the point of action.

There seems to be a dichotomy here that identifies two significantly different strategies. One, empowerment of the people. And the second, continuing empowerment of the central government. We've seen where success lies. My question would be, do we not need to make these two strategies both obvious, make the differences between the two, understand them, and

to study both the historical repercussions and— well, the historical results and the potential repercussions. I thank you.

DR. RICHARD H. SHULTZ: Well, I know a great deal about Anbar, and less about Afghanistan. I can say that at Anbar what was interesting was how the Marines were able to see opportunity early, well before the US government saw that opportunity.

So for instance, the initial meetings with the sheikhs occurred in the fall of 2005. Most people think that this didn't occur until September of 2006; it's not true. So the lesson there was to be flexible enough to understand where opportunity was in the environment.

I would agree with you completely, that in Anbar it was empowering the sheikhs who could then give you access to the people. That was the important thing. The sheikhs were the key. You had to be able to engage them. It means you had to, first of all, understand their place in Iraq. US policy was to write the sheikhs out, that they weren't part of the future.

So I would say that learning and understanding these two different approaches is very, very important. And my experience in studying Anbar is that the engagement element is absolutely critical. But it means that you have to really know who you're engaging, and that you can see in the way that – for instance, one month before we went back in 2006 – really built the engagement concept into the new strategy that General Zilmer had carried out when he got there. Thank you.

DR. JACQUELYN K. DAVIS: I just wanted to make a comment on the last question, if I could. I was just in Afghanistan, and it seems to me that we're fighting a different war across the country. Where the Marines are in Helmand, there's clearly an insurgency going on. And you need to operate according to counterinsurgency tactics. In the Kabul area and around Bagram, it's a different set of challenges. It's more like a criminal/drug organization, gang warfare, for example. And that's a whole different set of strategies that are needed.

And in terms of the governance piece, I'm not going to comment on whether I believe Karzai is a legitimate person to be supporting or not. But there is a problem with the central government in the provinces. We know that and we understand that. But the strategies, I think, are very different, and how you empower the local governments and the tribes, I think depend on the strategy you're enforcing.

I know General Petraeus understands it, I know General Allen understands it, because they've been talking about this publicly and privately, thinking about it in their planning. But I think we're at a point in Afghanistan where it's not just a straight counterinsurgency operation. That's my observations from a quick trip.

___: [3:08:16]

DR. RICHARD H. SHULTZ: Jacquie gets at the complexity of the environment. So one of the problems, if you look at a place like she described in Afghanistan, or in Iraq, you have different kinds of armed group challenges. So in Anbar, there was an insurgency, but it didn't fit the model of insurgency as we thought about it in the past. There were militias that were in Anbar as well, a different kind of actor. There were some of these criminal networks. So the issue of understanding the complexity of the environment then will mean how you respond will have to be tailored to the kind of threat and challenge you face.

ROBERT D. KAPLAN: If I could add. One of our conceptual problems is we tend to think of tribes and other militias as somehow pre-government or primitive. And therefore, we see it as retrograde, reactionary. There's actually a great book that counters this by Yale anthropologist James C. Scott, called, *The Art of Not Being Governed*. And he makes the point that tribes today, whether in Afghanistan or Iraq or Libya, and his example of the upland tribes of Southeast Asia, are not these primitive, pre-government tribes. They're very post-government in the sense it's a conscious rejection of central authority in favor of a more wider religious and cultural interest group, so that a tribe in Yemen may want to be more Islamic and reject the central government.

I've been in tribal chiefs' offices in the northwest frontier of Pakistan and Balochistan where the tribal chief is on his computer emailing people and settling divorces and distributions of property, and doing it all behind his computer, in a very modern setting.

Historically, even a figure like St. Augustine in the 4th century wrote that tribes serve a social good, because they contribute to social cohesion. We have to get away from our fixation with central government, that central government represents modernity, represents progress, so to speak.

DR. RICHARD H. SHULTZ, JR.: I think this issue that Bob raised in his speech and now has elaborated on here is really important. And that is the concept of central authority. So we often use this term ungoverned, but maybe the way to think about it is alternatively governed areas. In the case of tribes and sheikhs, they can be very sophisticated. There's this notion— I think it's very much influenced the way Bremer and the CPA thought about tribes and sheikhs. They thought about them as something that was ancient and not part of the new Iraq. In fact, they used to say this, that they're not part of the new Iraq and discounted them.

These were pretty sophisticated individuals, who understood many of the modern tools of society. So there's a danger in writing them off. Fortunately, the Marine Corps in 2005 recognized this, against US government policy. The US government's policy was that you shouldn't engage them, or you can only engage them in a certain way. And this is something that was interesting to me, the ability to the Marine Corps to learn on the job.

One of the things that I want to do out of this Anbar study is, I went back and I looked at all this literature on why and how organizations learn. It's very difficult to read, especially the business literature; some of it's almost incomprehensible. But I tried to deduce out of it what are six or seven of the things that all the smart individuals who've worked on learning have to say about what makes an organization learn. And then I'm going back through this Anbar thing and trying to see points in time where these characteristics are illustrated by Marine Corps action. And I'm finding some very interesting things there.

So this ability to not be paralyzed by conventional thinking is important. And I find that that was true in this experience.

DR. ROBERT L. PFALTZGRAFF, JR.: Thank you. Shall we now move on to another question? Please, right over here. And please wait for the microphone. And identify yourself as well, please.

DR. NADIA SCHADLOW: Nadia Schadlow, Smith Richardson Foundation. I have a question actually for Matt Devost. Your last point about capabilities and intentions, that's a concept that existed also, at least during the Cold War, if not before, but during that time. In a way, it was a lot easier. We'd look with satellites and spies and figure out how many tanks the Soviets were building and what they were doing. To a certain degree, we can do that in the cyber area a little bit with the Russians and Chinese. But how do you assess the capabilities in this area of non-state actors? And do you have confidence that we can even begin to do that? That seems to be a very different sort of problem in assessment.

MATTHEW DEVOST: It's very difficult. The way to develop the cyber capabilities is to go to Best Buy. There's nothing that we can watch for, there's no indicators, there's no key components we can put on watch lists like we could for issues like nuclear proliferation.

I think the best way to answer that is to get more granularity on attribution-related issues and get a better understanding of what's happening in the networks right now as an indicator of intent and capability. We're not going to be able to monitor the resources to be able to get that indicator or capability. We're going to have to watch activity.

The problem we have right now is that the adversary attribution is nearly impossible, even with a lot of the attacks that we see. I can't tell you how many organizations I've gone to that say, "We're under attack from China." And you go in and you look at it, and yes, it is a China-based IP, but you have to remember that China has the largest install base of pirated Windows software in the world. What's that mean? They don't get the updates, the security updates. Which means

they have these huge networks of compromised systems, and other countries and organizations and entities understand that and use that as a launch point.

So we really need to be able to figure out in these attribution issues, that might give us some insight into capability and intent, but we're not going to be doing it by monitoring the acquisition of resources and things of that sort.

DR. ROBERT L. PFALTZGRAFF, JR.: Would anyone else like to comment on the attribution issue? Shall we move on? Charles, Dr. Perry, Charles? And I thank Nadia for the question, because Nadia will be chairing a panel this afternoon. Welcome, Nadia.

DR. CHARLES PERRY: I just want to follow up on that question and turn it around a little bit in terms of our own capabilities, the intent capability side. We do seem to have an advantage here, and I just wanted to ask first Mike[sic], but others, too, is how you see we might actually creatively use our capacity to disrupt some of the scenarios we've just been talking about here. And there are distributed armed groups, criminal activities, criminal groups operating in ungoverned areas and urban areas, but how can we creatively, and perhaps even more specifically the Marine Corps creatively think about using the capacities we do have to counter some of these capacities that the armed groups have?

DR. RICHARD H. SHULTZ, JR.: It's a good question. I think there's one interesting campaign that— it's to study, but—

END OF 1009

BEGIN 1010

DR. RICHARD H. SHULTZ, JR.: —to me, it's kind of a model of how you would use this. Now, you might use this against Mexican cartels. Now, in the case of McChrystal, of course, his job was once you found them, to kill these people. And they killed a lot of them. So we may not want to be doing that in Mexico. But short of that, there was a very interesting way of attacking that network.

There's this mantra that everyone uses, it takes a network to fight a network. It's actually what he said. Or Arquilla said that first ten years ago, I guess. But that's a case.

DR. ROBERT L. PFALTZGRAFF, JR.: Yes, would you like to be the next questioner?

DAN POWERS: Dan Powers. I have the honor of being the lone Marine in the Navy N3/N5. I do strategic concepts, and I wanted to thank all the panelists for coming today. Mr. Devost, I see from your bio that you're recently— now you're a special government advisor to the Council and the DoD. My question to you is, as the military we obviously, and many organizations, have an insatiable appetite for bandwidth. And we deal with spillage and we deal with data being lost, and your anecdote about, would we be concerned about truckloads of stacks of sensitive papers or secret papers being shipped away. We would. And some of the numbers that we see nowadays are very conservative, I think. Is the way ahead for the US DoD, for maybe even the whole government, to move to the .mil and get away from just .mil?

MATTHEW DEVOST: That's a tough one. We want to put it in the constraints of the borders that we have, but then I'm also kind of a purist in thinking that no matter what network you create, it's always going to be vulnerable. I've made a living out of breaking into networks, and I've had a success rate every single time. Including when you're trying to breach classified networks.

So I think maybe the answer isn't creating harder networks. Maybe we need to start think about better approaches to the components on those networks. And as I mentioned in the presentation, I worry less about the network itself as opposed to the individual nodes. And I think there'll be technologies that we'll see here over the near term – and near term, I mean next five years – that will allow us to have open networks, but with components that don't respond to other nodes in the network unless there's some sort of authorization that takes place, before you even acknowledge your existence. And I've seen some of these technologies demonstrated, where if I'm authorized to talk to you, you'll talk back to me. If somebody's not authorized to talk to you, they don't even see you on the network.

So I think that's what we'll end up having, is kind of these secure components with the identity authentication and authority pieces being built in at the host level, and being able to operate on these mesh networks or insecure networks.

I think our tendency would be to further enslave the reality of technology's going to drive us towards more openness, and we need to look at how do we engage in protecting information in that context.

The needle in a haystack issue plays into that as well, too. It's being able to understand when is there anomalous activity on the network. If I'm sitting in the Middle East and I'm downloading 250,000 State Department cables, there should be some way to have an ability to notice that that is anomalous activity for investigation. There's got to be some components that we put in place that look at normal network activity and then determine when there's things that are out of spec that maybe a human analyst can take a look at.

So those are kind of the two pieces – hardening the hosts on the network, and then looking for the anomalies that exist within those networks.

DR. ROBERT L. PFALTZGRAFF, JR.: We have a few minutes remaining, and I'm going to give at the end of the time that we have, I'm going to give the panel members each an opportunity for two or three minutes of concluding comments. But what I'd like to do now is to aggregate the questions. So in other words, anyone who would like to ask a question, hopefully a few of you will still want to do that, I would like you to do so. And then the panelists can then note the question and think about the answer, and include it in their summary remarks at the end.

Now, I also have a couple of questions that I wanted to ask that I would like to put before the panel. The first is that one of our continuing themes, not only in this panel, but earlier this morning as well, has been urbanization and megacities. The term has been used a number of times. And here, another aspect of this is non-lethal capabilities, which were mentioned earlier.

It seems to me that when you talk about urban conflict, megacities, civilian populations, et cetera, you are necessarily thinking about non-lethal capabilities. And if the Marine Corps is going to play a role here, what kinds of non-lethal capabilities should they be developing in this emerging security environment? That's my first question.

And the second is in the cyber domain, and that has to do with another theme that we've been talking a great deal about, and will throughout this conference, and that is weapons of mass destruction, which leads to counterproliferation. And that made me think about Stuxnet and cyber operations as a counterproliferation tool. So would you include that, especially Matt, in his summary remarks.

Now, others may have even better questions than mine. So I'd like you to put them before the panel, and then we'll turn it back to the panel for them to give their summaries.

Yes, is that Dick Diamond? Dick?

DICK DIAMOND: Dick Diamond from Raytheon in Newport, Rhode Island. A couple nights ago I had the privilege of sitting in an off-the-record session with the Chief of Naval Operations, and he confessed that one of his top two or three worries was – [laughter] – as the resources for the Naval service were surely going to be curtailed in the future, what new allies and partners did we have to think about, and how did we build their capacity?

As I heard these very daunting problems that the panel talked about, it occurred to me no one talked about getting anyone else to do it. And when you think about the state out there, the nations that we have to go to are either going to be, half of them, weak, failing or already failed, that's not where you build partners.

So my question is, in the interwar period, as we're doing the strategic planning that Eisenhower found so useful, does America's expeditionary force in readiness plan to do it all alone? Or do you have some inputs from the panel on how you might create partner capacity and find new partners to help you with these very difficult and daunting tasks?

DR. ROBERT L. PFALTZGRAFF, JR.: And this, of course, is a theme that will be stressed in subsequent sessions of the conference as well. Other questions? Please.

CHRIS FALOFFICE[?]: Hi, Chris Faloffice of Naval Research. The question I have is a technological one, about autonomy. I'm surprised not to hear more about that, autonomous vehicles, robotics, et cetera. P. W. Singer at Brookings claims that we're at the dawn of a revolution equivalent to the railroads, the telegraph, the automobile, the airplane, whatever. I can buy these very sophisticated air/ground/water vehicles at Best Buy; what are the implications for an expeditionary force when this technology proliferates on a consumer level around the world?

DR. ROBERT L. PFALTZGRAFF, JR.: We have time for a couple of more questions. Yes, back here?

DOUG KING: This is for the whole panel. I'm Doug King from the Marine Corps. Ask all the panel members if you can give me where you feel the top region we should be concerned about, and why.

DR. ROBERT L. PFALTZGRAFF, JR.: Okay, one or two more. Back here, Jack? Wait for the microphone here. You told me to announce that, so I'm—

JACK KELLY: Hi, Jack Kelly, IFPA. Just wanted to ask Matt. Can you talk a little about deterrence in the cyber world and how that is shaping up in terms of developing a strategy for that? And how it may differ from traditional deterrence theory. Thank you.

DR. ROBERT L. PFALTZGRAFF, JR.: Anyone else? This is your last chance. Okay, well, then, we'll start with the panel. And let's go beginning with Matt and work our way over to Andy.

MATTHEW DEVOST: I didn't get to finish my notes, but we'll go off the cuff here. So dealing with a couple of the issues. On the non-proliferation issue, what is the role for cyber? I think there's huge intel role for it, in being able to understand capabilities that are being

developed, emerging. And maybe even leading to some ways to conventionally disrupt the development of those capabilities.

I don't see cyber as a legitimate means to deny proliferation right now. Disrupt, delay, understand, and maybe leading to the conventional methods to maybe deny, but I don't see cyber purely as a mechanism for being able to deny access to weapons of mass destruction.

On the autonomy, that's a great question and an issue that I spend a lot of time thinking about as well. I loved the P. W. Singer book that looked at all these new technologies and what happens when you get those in the hands of an adversary.

I think we don't know. I think one consequence is you start removing the human from the loop. You have less dependence on the human components in these operations, especially from the asymmetrical type threats, and the ability for them to automate and utilize these technologies to their advantage. If you can use your parent helicopter to deliver an explosive device, you don't need a suicide bomber. That's why the Terrorism Research Center, when we were doing our mirror image training, we were encouraging people not to just understand Al Qaeda, but understand the IRA, understand how these groups might move towards new methodologies and approaches and tactics. I think that cyber and availability of technologies is going to be another natural migration.

On the deterrence issue, again it's a difficult area. The deterrent components that we have right now seem to be just based on interdependence type issues, economic interdependence, a lack of understanding in how things will escalate. I know going back six or seven years ago, maybe longer, Dick Clark, when he was at the White House, would say, "Hey, we reserve the right to respond to an information warfare attack with conventional weapons, up to and including nuclear weapons."

But really, when we talk about these issues of attribution and being able to hide in cyberspace, is that really a legitimate deterrent? Do you want to be the authority that's pushing the button to launch the conventional weapons against somebody you think has launched a cyber attack

against us? It would have to be absolute attribution on that entity before that would even serve as a deterrent.

And is that something that the international community would accept? There's this huge discrepancy right now between cyber operations and the lack of the Moscow Rules that I talked about, and the use of conventional military force or conventional forces. We haven't seen a blending emerging of those two areas and the interrelations of those two areas.

That has huge strategic aspects to it. We need to decide for ourselves what does it mean in cyberspace to be operating? What are the things that we're trying to protect? And what are the objectives that we want to achieve? Then we can start thinking about deterring other people or the international norms associated with deterrence.

And then for my final summary, I covered, I think, my major points in the presentation. I think the one area of emphasis I would provide is that this topic has a history. We have had numerous studies and reports going back over 15 years, yet I continue to see the regurgitation of the same problems and same issues over and over and over again.

So I think it's important, and especially if you're trying to develop the forces within the different military branches, not just the Marines, that they have that context of history that's provided to them.

So that's key, having them understand the incidents that we've already dealt with, some of the strategic issues that have already risen and then move the bar forward. The issue that we have is that we seem to keep jumping over the bar at the same height from generation of expert to expert. There hasn't been generations, but from cycling of expert to expert, and people coming in and rediscovering the same issues, looking at new incidents in the same context as we looked at old incidents.

So I think that's a key piece. If there was one thing that I could emphasize is that as you move forward with understanding cyberspace or building an ability to operate in cyberspace, let's make

sure we keep the history in context. And there's only a 15-to-20-year history, but it's very important.

DR. RICHARD H. SHULTZ, JR.: There were a lot of questions, and I'm not going to try to address all of them. I think I'll address Dick Diamond's. It seems to me that these weak states are exactly where we have to engage. And the way that I've thought about this, and those who I worked with on this study, was that we need to develop the small-scale advisory mission capabilities for especially weak democracies, fragile states that have the kind of problems I talked about, but those problems aren't at the level of Pakistan or at the level of Afghanistan.

Now, sometimes you have a choice. You get Afghanistan and Pakistan and that's the way it is, and that's a heavy-duty mission. But in many of the places where we have interests and where this weak state problem is growing, we can engage and maybe be a bit pre-emptive. Now, that means that we have to have the ability to help build local capacity.

Local capacity is something more than just what the Marine Corps could provide to this; it involves civil agencies as well. But building local capacity through engagement for local security forces means a capacity to be able to deal with the kinds of challenges that they're going to face.

And so, this advisory capability has to be built on skill sets that help them deal with irregular challenges. And non-lethal is part of that. But this is an engagement that's tailored to the irregular threats.

So to me, that's really important. And it's something that the Marine Corps has had a lot of experience with, not just recently. And so it seems to me that, from the point of view of engagement, to build security force capacity that is tailored to the irregular challenges, the Marine Corps is a really good organization for that.

What area is going to be the most important, that's the only other question I would answer. I think that given the earthquake that's going through the Middle East, that we have to really focus on that. And why and how that's coming about, we don't understand, but it's coming. And we

have such huge interests in that region that, to me, that's going to still remain one of the centers of gravity. Not to take anything away from what you say, Bob. To me, that's a big area that we're going to have to be engaged in, and we have to learn about it.

ROBERT D. KAPLAN: In answering some of the questions, let me focus on something that we partially neglected during our presentations; that's big powers. We spoke about collapsing, weak powers, but big powers. Look at East Asia. East Asia is the center of the world's economy, but also increasingly of world military activity. East Asia is not a matter of primitive land forces, of irregular forces. It's not just China, but Japan, Vietnam, Malaysia, Singapore. The Indo-Pacific is becoming a realm of real civilian military, post-industrial complexes with air forces, navies, cyber capabilities, et cetera.

In other words, 30 years of rapid economic growth is leading to the most sophisticated kinds of military growth. It's not just China that seems to have a shop-till-you-drop policy towards the acquisition of new submarines, diesel, electric and nuclear. The countries of Southeast Asia have increased their defense budgets by a third over the last ten years. Vietnam just acquired six new state-of-the-art Kilo class submarines.

And when you look at East Asia, let me say something about China. China is not only moving outward into the first island chain and beyond as it becomes a maritime power. It's building state-of-the-art deepwater ports along the Indian Ocean in Pakistan, Bangladesh, Sri Lanka and Burma that won't be military bases, per se, because that's too provocative to India. But they will be part of like a maritime trading empire, kind of the 21st century equivalent of 19th century British coaling stations, that China is going to have all the way from East Asia to the Mediterranean.

And there was a question of, what can we do to get others to help us? Every time Japan and India sign an accord, or there are more interactions, political and military, between Indonesia, Japan, Vietnam, India, we win, because it gets all these Rim-land states to kind of— where leveraging in most cases like-minded, democratic others to help — I'll put it delicately — to help manage the peaceful rise of China in that sense.

And then just one more point. Because of our experiences in Iraq and Afghanistan, the US military, particularly the Marines and the Army, have developed this incredible intellectual capability of dealing with counterinsurgency, irregular warfare, dealing with sub-state actors, and all that. And because we have this nation-building capability, there's a real danger in it. And the danger is, when the next place collapses, there'll be all this pressure on us to do something, to get involved.

We keep saying we're not going to put boots on the ground in Libya, but in a post- Gaddafi world, where there's no central authority in Libya, or something, there's going to be all this pressure on the US to use its nation-building capacity.

And so, part of the challenge is going to be to resist that. I'll be very frank. Because we're entering an era, as Andy said, of rising threats, but lowering budgets. And we really have to pick and choose where we're going to get involved.

Thanks.

DR. ANDREW F. KREPINEVICH, JR.: Just two points. One is the point on robotics, and again I think that's one of the interesting emerging areas of warfare. It seems to me there's a competition here – the better you can preserve your network, the dumber your unmanned systems can be, because you can remotely control them. But the more fragile your networks, the more artificial intelligence you have to build into the system.

So the big question is, who's going to win this competition over time? And the answer to that question will tell you a lot, I think, on how fast and how far robotics are going to take us.

And along those lines, my sense is that it may be, in the short term, more difficult for us, since we haven't really thought a lot about our battle networks and how to protect them, that may make it more difficult for us.

And what I would say in general is, if you look at the proliferation of guided weaponry, nuclear weapons in the developing world, and the diversion of resources I think that's going to come with the maturation of the cyber threat, we're going to be talking about a less permissive, higher cost kind of environment when you're talking about power projection. And that, I think, combined with Robert Kaplan's point about the growing competition among major powers, I think could find us in a world where we do a lot less overt power projection and are engaged a lot more, both ourselves and our rivals, with proxy warfare. And to think about that, especially in the developing world.

The other point is with cyber. Somebody mentioned cyber as a counterproliferation tool. What concerns me most is cyber tools as a prospective element in generating catalytic war. And let me just very quickly; assuming you're wrong, it's nuclear weapons. Missile flight times between Israel and Iran are six minutes. There are at least reports in the open literature that the Israelis Windexed the Syrian radars back in 2007 when they went after the reactor site. There could be a third party some years from now that doesn't Windex the Iranian radars, but actually shows them they're under a massive attack by Israel.

If you have six-minutes' response time, what are you going to do? We don't know. We do know in '79 and '83, both us and the Soviets thought we were under a large-scale attack. Fortunately, we had the luxury of 20 to 30 minutes to figure things out. If we had had six minutes, I hate to think; I probably wouldn't be here to think.

The other thing in terms of cyber deterrence, we have this anomalous situation right now where we saw our strategy is deterrence. We can't, as Matt pointed out, necessarily threaten retaliation because of the difficulties in attribution. So if you've got that problem then you shift it, it turns to denial[?]; we'll convince you that we can stop your attack. Well, again, we've pretty much left the dotcom world to fend for itself. It's not quite clear who's going to prevent this attack from succeeding.

And then you get into the issue – and this is the final thing I'll say – if you're looking at somebody who's contemplating an attack, you have a proliferation in the number of potential

players. If Matt can get into any network in the world, then there's probably a lot of people who can do that. Not thousands and thousands, but a lot more that can hit you with a nuclear attack. Point number one.

Point number two, people like Hitler and Saddam Hussein, and some of these other folks even, that are responsible for states, are highly risk-tolerant. And you add to that the potential for non-attribution in an attack and, again, you wonder where things might head. And then finally, non-state entities, what are you going to retaliate against? What do I have that you can go after that you're not already trying to go after?

So I think this is a very troublesome area, and I think the sort of thing that Matt says, in terms of really taking a serious look at what's going on here couldn't be more important and timely.

Thank you.

DR. ROBERT L. PFALTZGRAFF, JR.: I would like to thank all of the members of the panel for their outstanding contributions. And if you were pessimistic about the situation before hearing this panel [laughter], I don't know what you will be now. But you should at least mitigate that pessimism by having lunch, which is outside. It's a buffet lunch. You should get what you wish, bring it back in here. The silverware is all set up here, as you can see. But sit down and enjoy your lunch, and then we will have our luncheon speaker, Congressman Akin.

So this session is ended. And again, many thanks to this panel for its outstanding contribution to the conference. [Applause]

END OF SESSION 1