



Mitchell Institute for Airpower Studies

Presentation: "The Rise of Cyber War"
AFA Global Warfare Symposium, Los Angeles
November 18, 2008

Rebecca Grant, Director, Mitchell Institute

Moderator: Our next speaker is a distinguished author, a writer and researcher. She's a Senior Fellow of the Lexington Institute in Arlington, Virginia; and the Director of AFA's new Mitchell Institute for AFA. She has worked for the Chief of Staff of the Air Force and the Secretary of the Air Force. Her complete bio is in your program.

Please welcome to the stage Dr. Rebecca Grant.

[Applause].

Grant: Good afternoon. It's always good to get to speak after the coffee break. I hope everyone is ready to dig into a session beginning with a talk about cyberspace. The Space Command guys are here! What they're really happy about is I said that probably they should be the ones to come up here and speak about this because of the changes about to take place within the Air Force. I think you'll see these fellows having a lot to do with how cyberspace unfolds.

But what I'm going to do for the next half hour or so is give you a much broader and theoretical look at where we stand in cyberspace.

Let me start off by quoting from some names that should be real familiar to you. I'm going to start with Deputy Secretary of Defense Gordon England. He made a remark this spring. He said, "Cyber warfare is already here." As far as he's concerned, this is an arena that we are dealing with now day to day.

Another gentleman you've heard of, the Secretary of Homeland Defense Michael Chertoff. He has said, "The reality is that cyber attacks are not decreasing. They are increasing. They're increasing in frequency, in sophistication, in all the things that we worry about most."

Finally, from General Kevin Chilton who says, "I firmly believe we'll be attacked in that cyberspace domain." He goes on to say, "Our challenge will be to continue to operate in that domain."

What I'm going to talk to you about today is how this domain looks. This is probably the most famous picture of the Air Force executing things in cyberspace. You've seen this

picture all over the place. What it really tells us is that across the last decade cyberspace has become an essential integrating medium for air and space and all the domains that go with joint warfighting. But the fact of the matter is, we are living in exciting times. It is not easy to articulate a new domain of warfare. It is particularly not easy to pull together this cyberspace domain that is, as the quote says, not necessarily a thing or a place. So how do we grasp what this domain really is?

If we look back at the last two domains that have emerged, the lessons are very instructive but they tell us it's going to be a really rocky road ahead.

This picture here shows a particular point in time of the emergence of the air domain. Of course the other domain that's emerged in the late 20th Century was the domain of space. But let's talk for a minute about what it took for airmen to make this air domain emerge.

This picture was taken in the summer of 1921. You see there a bomber. It looks like a pretty formidable craft. There are two individuals there talking earnestly to one another. One is General William Mitchell and the other is a man who had been newly appointed to be the Army Chief of Staff, General John Pershing. John "Blackjack" Pershing, as they called him.

Even though we don't know exactly what they're saying to each other, the sense of the conversation is pretty clear. In fact this photo was taken at Langley Air Force Base. General Pershing, who had only been Chief of Staff for about a month, had come down to see what Mitchell was doing in conducting tests of aircraft against battleships. He'd been working with the Army and the Navy over a period of months to see if aircraft could attack ships at sea. Mitchell is enthusiastically explaining to him what they're going to do, what they've practiced, what their tests are hoping to show. In essence, what this domain is going to be all about.

We can't quite see Pershing's face, but I think we know that there's a little skepticism here. He's seen air power and its uses in World War I. He knows Mitchell quite

well and understands that this is someone he needs to listen to. But the question about what this air stuff and this weird looking airplane behind him is really going to amount to is very unsettled at this point in time in the summer of 1921.

In fact this domain remains a bit unsettled through that inter-war period, and it really takes the experience of World War II to articulate what the air domain is about, why it's important to joint warfighting, and how it leads them after the war to the birth of the independent Air Force.

What this tells us about cyber is that we have a ways to go. What I'm going to talk to you about today first of all is that there's an important difference between the cyber and the air domains.

The cyber domain is not just a matter of breaking off an established and proven mission out of one service and creating it into something bigger, nurturing its technology. There are interagency players, I'll talk a little bit about those to get a sense of the landscape. There are big questions about how we define the domain. And finally there are questions about what it all means for the Air Force.

Unlike the picture of Mitchell and Pershing what we see in cyberspace today is an already well established set of government players. We want to call them interagency players. A bunch of their office symbols and departmental seals are put there. And yet if you look carefully at the lines of authority and the budget lines, what you see is that most of these lines go back either to the Department of Defense and land somewhere on the Secretary of Defense's desk; or they go back through to the Department of Homeland Security.

And yet what this tells us is that for the first time we are dealing with a domain that is well established in areas outside of the pure military arena, and in fact in the case of homeland security, outside of government control.

The Department of Homeland Security has taken on a pretty big role in cyberspace in the last couple of years. The classified combined National Security and Homeland Security Directorate that came out earlier this year underscored that role. Yet what the folks at Homeland Security will always remind us of is that while they have a mission to help secure cyberspace and that infrastructure, they don't own this infrastructure. Ninety percent of so

of it is in private hands. Homeland Security's mission, a big part of it, is to educate and increase awareness.

They're also very clear that they don't engage in the same types of intelligence gathering or network operations that one would see in a military department. Nonetheless, Homeland Security is a major player here and one of the first places that we think about when we think about defining security in cyberspace.

Of course the other major player is the Department of Defense. Here there are many many many pieces. This in some ways is what is so unique about cyberspace. You don't have a small group of what was once the Army Signal Corps out experimenting with airplanes and trying to figure out how it works. You don't have a small group understanding space launch and how that works. What you have is a much broader set of relationships. Some of them go back quite a long way.

Let's take, for example, the National Security Agency whose lineage goes way back into the early part of the 20th Century but whose formal role in cryptology and information dates from the 1950s with the agency in its current form.

What we have even within the DoD controlled cyberspace arena is a number of different missions. Some centered on intelligence and intelligence exploitation, others centered

on assuring the network, providing it to warfighters in a tactical, operational sense, and still others centers on learning ways to exploit and use the networks in attack operations.

From a pure organizational perspective this is not an entirely satisfactory situation. The last couple of years have seen some major moves and efforts both within the services and across DoD to clarify lines of control. One of the biggest of these, of course, has been to confer a clearer mission on STRATCOM. To place it first a couple of years ago, and the integration of cyberspace into the global mission of STRATCOM has done quite a lot to clarify the roles.

Yet that leaves open a question too of where the theater commanders fit in. If you have a regional commander who requires some type of cyberspace capability, is there a potential conflict between that regional commander and Strategic Command's global mission?

These are the types of military questions that we've asked and answered in other domains, and we are still

asking and looking for answers to these within the cyberspace domain.

Again, quite a lot of progress in the last few years but it leaves an overall question about who the players really are that make up this domain.

Fortunately this is an issue that has really attracted the attention of our most senior military leaders. I wanted to put this picture up here showing Admiral Mullen, this picture was actually taken when he was CNO, and in a way he's a little bit like the old, old picture of General Pershing who was out there looking at Billy Mitchell's bomber saying what is this? What's this supposed to do? I see a little bit of that same look on Admiral Mullen's face.

But in the discussions where he's talked publicly about cyberspace, he's pretty clear about a couple of points. One is that they don't have all the answers yet. Another is that there really is a significant threat here and that it's worth plunging in and trying to figure out what the right answers are. And whatever those answers are, they have to look a little bit like the way you do business in other domains. You have to nurture your younger airmen, for example, who work in this area. You have to bring the leadership perspective in. The older generations have to learn what this is all about. Yet we still see a level of uncertainty here I think at the highest levels about how we want all this to play out.

Indications are that one of the recent Roles and Missions Reviews that was done has in a way said look, cyberspace does belong to all the services. We're not clear yet on where we want this to go. Certainly there's a strong case to be made there, that each service should work to assure its own network operations and connectivity but there may be still larger questions about this warfighting domain.

I think the key questions for DoD boil down to how you fight this domain. What you really want the joint force commanders to do. How they divide that inevitable tension between intelligence collection and operations. We've seen it in other domains. We'll see it very clearly in cyberspace too. And how you nurture this domain.

But in the next section of my talk I'm going to go even more theoretical for about six or seven slides and try to give a sense of why we struggle so to understand what this cyberspace domain really is.

Let's go back to this picture which I'm very fond of. As I said, taken in about 1921, so this is roughly if you date it from the earliest experiments at Kitty Hawk, this is a good 20 years into looking at the air domain. This picture was actually taken, obviously, after World War I, after there had been extensive production funding, build up of air forces, use of air forces in combat. And yet airmen were still a long way from having mastery of that domain and from having it understood in a budget and policy sense. From having the real doctrine of air power completely understood.

Let's compare that to where we are with the cyber domain today. I like this quote in the center of the left hand column from Billy Mitchell because he had something to say about everything, as it turns out. But in this case he talks about the rapidity and sureness of electrical communication. You see a little foreshadowing of what cyberspace means to us today. Yet there's caution here because if we wanted to we could go all the way back to the dawn of the electromagnetic spectrum, to its exploitation in the Civil War with the telegraph and other inventions.

To me, the electromagnetic spectrum is a central and crucial starting point for defining cyberspace, but it's not enough all by itself. The physical spectrum alone does not define that domain in isolation. Otherwise we really would be dating it from a much earlier time.

To me the more relevant dating begins several decades ago as shown in the orange box. We look at the creation of ARPA that helped to foster some of the early concepts and technologies. By the 1960s there were companies that were working in long distance computer networking.

The internet as we know it today emerged in its clearest form in the 1970s. By the 1980s there were military networks exploiting it. We saw an expansion of commercial networking as well.

Then of course the 1990s brought about the revolutions that brought this domain out much more broadly. Both the World Wide Web, the changes in desktop computing, the things that created both the larger infrastructure and our ability to use it in day to day tasks much more effectively.

As this decade, our first decade of the 21st Century draws to a close, we've seen even

further evolutions and hints about more to come. I would cite, quite simply, cloud computing as another evolution in what this network and this domain will look like.

So what we see here really is a question about the value that we assign to this domain. You can't look at any single date on that chart and say all right, bang, there it is. 1968. That's when this domain begins. You have to look more at the value, the utility, to find the definition of this domain.

That gets me back to the picture that was on the opening slide. It's perfectly normal for us in Western culture to debate about what a domain really is. In fact I will assert, without taking too long to make this case, that our discussions about cyberspace are merely the latest flicker in an ongoing series of attempts to understand what's real and what's false. It goes all the way back to Socrates. And that's who's pictured there in the sort of olive drab toga there. This is a detail of a painting, actually a fresco in the Vatican called "The School of Athens". For any of you who know the work, this is actually a very tiny piece of it. It was done by Rafael and he lined up all the great thinkers of the day and of previous ages, and of course the center of it really is Plato and Aristotle. So Socrates is stuck over here on the left.

What's interesting about Socrates was that he didn't write it down. It was Plato who wrote down everything he said for the most part. I think that's why we see Rafael depicting him here as doing a bit of haranguing of one of the other philosophers. I think that chap on the left in blue is supposed to be Parmenides. But again, this image tells us of a particular symbolic value that's very important to how we think about cyberspace.

That is the value of the discourse and the discussion that goes into it. It's really a concept central to all Western philosophy.

To a great extent we believe and understand what we say we believe and understand, and you can go back to Philosophy 101 and read all about this. But what it boils down to for us is that when we assign value to these virtual transactions, we create a domain, a cognitive domain, that we all agree has value.

Does cyberspace meet that test? Well, a good way to look at it is with the criteria here in the gray box. You could say that the criteria for a domain include richness. What's the value and significance of that domain? That's why back when Billy Mitchell was haranguing John Pershing and theorizing about rapid electrical communication it really didn't meet the test of any sort of domain. It

wasn't of enough value or significance in that period of time.

Second reason. There wasn't enough persistence. For those of us old enough remember, the earlier days of the type of e-mail that you would have had at a university say in the 1980s, it was a very small part of what you did. The persistence of this was not a major portion of how you conducted your research. It's taken the developments of today to bring us up to the point where the combination of storage and utilization and the

continuity of that gives us something that we rely on more and more every day, it seems.

What about connectivity? When did cyberspace become your first choice of communication? Not so long ago. And yet whether we look at our personal communications, our business communication or the use of chat to help organize operations in a theater of war, we can see that that connectivity is there and that cyberspace meets that criteria.

And the direct interaction, where the gains outweigh the costs. Again, something that I think for the most part we have all well overcome and we can say that cyberspace is a rich domain, a cognitive domain. So this is more than just saying because we can occupy and dominate parts of the electromagnetic spectrum. That, of course, is a key and crucial distinction. Without that we don't have this discussion, we don't have the dialogue, we don't have the richness of the domain. But in the end it is the value, the persistence, the connectivity, the utility that defines this domain for us.

What does that mean in the military sense? I think you can boil it down pretty simply and say we know this is a domain because we all use it. Because we hear Deputy Secretary of Defense Gordon England talking about the persistence of cyber attacks. Because this has come into the dialogue. So we see it as a cognitive domain. Quite normal that we will continue to struggle with the concept. That's what the tie to Western philosophy tells us, that we will continue to debate where the edges of this domain are. I will speak in a moment about why that is crucial in our policy discussions.

But let me close my little art history lecture with a couple more images. These are some of the most common images you'll see in cyberspace. There's the photo again that I used in the beginning. The image on the far left is one of a number of similar types of images that attempt to depict the connections of the internet. But I would ask

you just for a moment to step back and see what these images are trying to tell us. They are trying to show us either the web itself or the people who are using it. So I would contend that these images are part of our attempt to visualize and define in our own minds what this domain is like. Again, because we carry it through in this dialogue we can tie this right back through Western philosophy and say that yeah, we do sort of have a reality check about how we visualize this domain and what it is. So any time you see some of these images again, keep that thought in mind.

I said this tie to what the domain was and what it meant and how we debate it would have a policy link. On this slide I will try to make that link for you.

Most of our policy is based on yet another set of principles derived from Western philosophy, from practice, from agreements and events occurring much more recently than the time of Socrates. So we understand what the anarchical system is. We understand what is within the domestic bounds of the state, we understand what is the international system, and we have rules and procedures based on our common understanding of all that.

What's tough about cyberspace is that it up-ends and unravels some of our understanding of what this global commons really is. And so while it's easy enough over a period of centuries to understand how sovereign states should act—either on their own; when there are interventions in each others affairs that are justified; when they aren't; how groups of multinational states will act; how a United Nations will act. We have all these structures in place. We may debate them, we may disagree about them, but the forum for discussion is very clearly set.

What is tough about cyberspace is that that core of sovereignty gets questions. We're not as clear on where the boundaries are. We're not as clear on where the protocols differ. This is why you often hear analogies between cyberspace and the development of the law of the sea. As we know, pirates and privateering were really big business sanctioned by major governments for a very long time, right up through the middle of the 19th Century until agreements reached in Paris, of course, set some different standards for privateering in particular.

So we know that this global commons of cyberspace is going to be a difficult area for us as we go through. We're still struggling to find the domain, to understand its boundaries, so we are looking for that new nexus of value that can translate up into our understanding of

international policy. To put it more simply, what constitutes a breach of international protocol? What's an attack? We're under attack all the time, why aren't we responding? These are the types of questions that we have to struggle with a little bit more to fit into our current concept based on a different sense of the global commons, a different sense of sovereignty, in order to understand what our future policies in cyberspace will be and what our freedom of action will be.

Is there any hurry about doing this? I would say if you want to know the answer to that question just ask Estonia. After the denial of service attacks that occurred there last year, went on for about a three week period, the Estonians really made this a major international issue. They went to several of the international forums, discussed this, it became a big discussion item within NATO. The NATO member states were not all of one mind about what this all meant.

Admittedly, Estonia was a unique case in some ways because it was a very very connected society, a small state, and yet this is exactly the sort of thing that we see is possible now. This is what our leaders in Washington are talking about when they say these attacks are increasing, the attacks are ongoing, we are already in this environment.

I think General Cartwright put it quite well when he said straight out that Estonia was a wakeup call. What this means is that we don't have too much time to begin to figure out where the policy boundaries lie.

Now NATO and others have taken some steps to clarify what this all means. The

Estonians have set up a computer response center. Things are moving forward. But Estonia points out clearly that the [... blank spot on tape ...] means, based on our older definitions of the global commons, we can't rely entirely on our heritage of international law to bring us through this. It will be a source of debate.

So these are the big questions that we're left with. Who sets these cyber rules? Quite a lot of what goes on on the internet is governed through international protocol that really does not revolve around a state-centered focus. You can make analogies to other industries and other periods in time where this has been true, but quite a lot of this is governed by supranational consensus, if you will.

I mentioned earlier the role of the theater commanders. How do we see their needs in operating in cyberspace? How do they track with other domains and with other commanders? What are the roles of the services? Each of the services today understands the importance of cyberspace but has really quite a different vision and quite different organizational setups for how this will all unfold. And finally, again, so much of this responsibility comes neatly back to the Office of the Secretary of Defense.

The Department of Defense as it's set up today has quite a lot of ability to sort through and solve the various rules and regulations that pertain to this and to arbitrate between the interests, and most importantly, to give us more of a vision for looking forward.

Just to add one more layer of complexity, this is not an area where we can say the United States has complete dominance. This is not quite like looking at our air and space dominance capabilities and saying hey, we've got a lot of time to figure this out.

Some have asserted that the U.S. is already behind. Others have said that there are peers already here and functioning. I think we can certainly see who some of those peers are. Some of them are our allies. Some of them are competitors. But the fact remains that the barriers to entry in cyberspace are a bit lower than they are in some other areas, so we are already dealing in an environment of multi-polarity.

We may see this more as the next decades unfold in other realms as well, but in cyberspace we are already dealing with a multi-polar world. It makes it that much more critical to understand what this domain is, how the rules are set, and where we want to go with our vision and policy.

Somehow to me it all boils down to this task of safeguarding the commons. So I had to stick in just one more picture. This is one of the Broygles, I can't remember which one, and it shows actually I think a festival taking place as the cross-over between Mardi Gras and Lent. But I like this picture here because it shows what we most want out of the commons—the ability to interact, the ability to have commerce and enlightenment, and it points out exactly the kinds of things that cyberspace has already given us and yet which we must learn to guard within cyberspace as well.

We already know we can't do it just based on how we define states and how we've done

that in the past so we will be struggling to secure this domain. We will be struggling to secure something that was designed to be open and inclusive.

We've already seen some of the difficulties with that and I think we will continue to see them.

Finally, I want to wrap up with just two slides that bring it back a little bit more to what this all means for the Air Force. I think it was General William Lord who said that the Air Force didn't just stop when the Secretary of the Air Force some time ago declared that cyberspace was part of the Air Force mission. To fly and fight in air, space and cyberspace. That wasn't done in a random way and it didn't mean the work was done. In fact it meant, said General Lord, that the work was really starting in this case.

I opened the talk in part by talking about how important this integrated medium has become to everything that we do in joint warfighting. It's particularly so for the Air Force and you can say in a way that the Air Force has the most to lose in this arena. I think that's why we've seen such bold and steady steps towards exploiting the cyberspace domain by airmen.

I was a little discouraged to read some of the pundits in the press through the summer that talked about how cyberspace was a grab by the Air Force. It seemed to me rather that it was an attempt to sort out the people, the budgets, the organizations, that already constitute a large and thriving mission. So I'm glad to see the steps moving forward with AFCYBER with the numbered Air Force and all that we will see unfolding in the future and which you'll hear much more about from others throughout the conference.

Yet we still come back to some of the same questions. If anyone needs this it would be the CFACC who needs to understand where the policy boundaries lie, where the differences between STRATCOM and a theater commander lie. What the possibilities are. And you'll see CFACCs dealing with an age-old tension that between operations and intelligence. To what extent do you want to listen on a network? To what extent do you want to use that access to accomplish effects?

Somewhere down the line a CFACC will face a decision. Do you want to just confuse a surface-to-air missile and that system? Or do you want to destroy it? Those are the sorts of things that the cyber domain will bring up and

here our policy must take into account not only what the air component can deliver, but what our allies bring as well.

So for the CFACC of the future, cyberspace remains an extremely important domain and one where airmen will have to work through and bring many of the solutions to the table for the benefit of the joint force.

Concluding observations. I couldn't resist again showing this picture of Socrates because I think one of the most important steps here is to continue the dialogue that is already

well underway about what cyberspace means. You'll hear later, of course, from General Chilton who's pictured there at the bottom. I wanted to put these two images together to stress the importance of working through this domain and the dialogue that we have here.

We really do have within DoD the ability to do pretty much whatever we need to do to sort out the policy in the domain of cyberspace, but it's very much going to be up to airmen to articulate their vision of how cyberspace fits across the domains; their vision of what cyberspace does uniquely; and of what it will do for our national security.

Cyberspace has already become a wonderful domain of commerce and of enlightenment. Unfortunately it will become a domain of conflict as well. But I think if we have steady guidance from the Air Force and across DoD that cyberspace will become a rich and important and thriving part of our national security and of our national way of life as we go forward in the 21st Century.

Thanks very much for listening.

[Applause].

Moderator: Thank you, Dr. Grant. We do have time for some questions. On the last break somebody jumped me and handed me one of these and said if you only get to ask one question on this are, ask this one, so we'll start off with this first question.

Dr. Grant, if you were an advisor to the Obama administration to sort all this stuff out, how would you attack the organizational issues? And what one, two, three policies would you try to implement as a first order priority?

Grant: First of all, if I were an advisor to the Obama transition team I think I wouldn't be allowed to show my face at this point because they've really kept themselves quite hidden away. But your question is a very good one.

I think probably the first, not so much for this audience, but more broadly, I think the first issue is awareness. There's a real question about understanding where the players are within the government. I've given just a little sketch of how that is but it requires a much much more detailed look. So I would say probably the first overriding question is extending awareness of this and how important is it.

I think to me the second one that's also very important is really straightening out what role we want our military services to play over the course of the next several decades. We have come to a point where our definition of the domain and our dealings in cyberspace are so spread across a number of agencies that we're really facing a question of whether we want this to be a uniformed task or not. To what extent do we want those in uniform to lead this area?

My personal view, if I were giving advice to our President-Elect, would be that the uniformed services ought to have a bigger lead in this than they do today.

Moderator: You mentioned awareness as an issue of this domain. There are some writers that have said that this area is shrouded in secrecy and that whenever there's a robust discussion of the policies or any changes that need to be made at the national level, even of the tools that are available then it's immediately into the classified area. Others also draw this same parallel to some of our operations in space. It's not just in this cyber area.

What would you do in terms of opening up some of the veil of secrecy behind this?

Grant: That's a great question and I can see the whole front row here sort of shuffling around. What do we do about this veil of secrecy?

Well, I think we do need to open it up a bit more. We've dealt with highly classified matters before, highly classified technologies. I think we've found in other domains a way to not talk about the things we shouldn't, but to have a broader dialogue about the things that we should talk about. I would really urge a bit more of an opening up of this domain so that more of the policy community and more of the nation can come to understand

what it really is. So I hope we will see it open up a bit more in the future.

Moderator: If you were the Commander of AFCYBER, what would be one or two or three steps you would take to start to attack the Air Force's role in this area?

Grant: I think most of those steps actually are already underway. I'm really delighted to see real progress in Air Force doctrine on cyberspace which I think is very close. I think the AFCYBER crew, if you will, have done a good job in understanding their budget requirements. I think I'd challenge them to say do you really have the funding that you need going forward? I think they've done a good job also in building the processes to nurture this as a career field which will be absolutely essential to whether it thrives or not in the future.

I'd like to see it become a bit more of a roles and missions discussion but without the terrible baggage that we so often bring to that. I'd love to see cyber type of warfighter talks as we have seen the services do, the Air Force and other services do across other domains. But I think AFCYBER's doing a super job and they've got this under control.

Moderator: Could you address the non-state actors and the role of national governments in regulating their operations and enforcement of multinational rules within cyberspace?

Grant: A great question because this goes right to why this is so very difficult, and whether those non-state actors are terrorists who make use of the communications

advantages of the internet, or whether they are criminals in other parts of the world who are breaking into the financial system and going after the accounts payable, you have some very diverse actors. The fact that these are real problems that we deal with day to day has made the challenge of understanding how to secure cyberspace that much more difficult.

So I would like us all within the next few years to have parsed our understanding of that so we understand what the terrorist-related problems are, what the sort of criminal-related problems are, and then what the peer competitor and nation state problems are.

Moderator: Given the importance of cyberspace and the need for some kind of control of it, in your opinion what will it take for America to gain, and is it even possible to gain superiority in cyberspace?

Grant: First of all, I think we need to spend some time defining that. I would go back to your initial question about advising the new administration. It would be great if within the first term of that administration we understood and had a clearer definition of what superiority in cyberspace really meant.

I think one great marker that has been laid there is the ability to continue to operate. That's been stressed, whether from General Chilton or General Elder or several others who have talked about that. Clearly, the ability to continue operations is a mark of superiority in cyberspace, just like it has been in air and other domains as well. But we have a ways to go in understanding what that means and how to achieve it.

Moderator: The last question is, sorry we don't have time for more. I'm sure you could wax eloquently for hours on the subject.

Grant: Hours. [Laughter]. You and I together, we could go for hours. [Laughter].

Moderator: The last question is, you mentioned the Department of Homeland Security's role in defending America in the cyberspace domain, but they seem to be not even hardly even organized. How long do you think it will take them, or is it even possible for them to make enough progress in this area to make the average American feel safe?

Grant: That is a question that could definitely be discussed for hours.

They have a very tough challenge because so much of what they do is about spreading awareness and trying to get entities and groups that they don't own to do things in a certain way. But I think they're making some good progress actually in making us more aware of what the requirements are. I think their public information campaigns are good. I think they'll need to find a way to work with different industry groups, whether that's banking and finance or others, in a way that helps those industry groups with their challenges. So a lot of ombudsman work there on the Department of Homeland Security, but I think they are making some progress.

Moderator: Dr. Grant, time's run out. Thank you very much for a very thoughtful presentation.

[Applause].

I have to tell you that Dr. Grant is the author of not only the first but the second Mitchell Institute study and we've brought with us about 500 copies of the study, so when you go out on break it will be out in the break area and I'd urge everyone to take one and read it and absorb it. Thank you very much.

Grant: Thank you all.

END TEXT