

General James Cartwright
Vice Chairman, Joint Chiefs of Staff
*Cyber Strategic Inquiry Enabling Change Through a
Megacommunity Strategic Simulation*
Washington, D.C. -- December 18, 2008



Chuck Boyd

General Cartwright, Vice Chairman of the Joint Chiefs. Known and respected by everyone who's been around him in any phase of his life. A Naval Aviator. Actually a Naval Flight Officer before he was a Naval Aviator, starting out in about 1971 as I recall. Made the transition. And this is inside baseball, but I know that game. That's not an easy trick. And after becoming a Naval Aviator—and this is what really rings my chimes—this Marine became the Naval Aviator Carrier Aviator of the Year, which I'm sure made a lot of Navy officers upset.

He did everything that anyone could do in that world of aviation. Commanded at every level. And then rounded out a career with some experience at hard stuff. Resource allocation. J8. Running a COCOM. A strategic command. A man who Admiral Mullen described to me before I had had much experience with General Cartwright as a true strategic thinker. The only General that I've run into, and that probably tells you a little bit about my age, but I think nonetheless a pioneer. The only General I've ever heard of that had his own blog. And with a call to action from troops who work for him irrespective of rank or age that if you've got the answer to the question, I want to hear it. An openness that is I think exemplary in a profession that's not always the case. And an example for everybody inside and outside of government.

Enough of me. General Cartwright, thank you for joining us tonight.

General Cartwright

This speaking to you while you're still armed is dangerous. Oh, that's good. Nobody's out there because I can't see a thing.

I think the ROE tonight is 15-ish minutes of me. We'll treat this as a chandelier, so I'll say "stimulating you" rather than the Marine axiom that I might use, "piss you off." And then we'll turn it around and you can come at me, and we'll go any place that you want to go.

But this is an area that for me has been a passion. I'm not a technocrat, and I would have trouble discussing this at a really technical level oftentimes. But for me and I think really for this nation, this cyber/Internet/networked activity Information Age is so leveraging and so important to this nation. It is pervasive in our business. It is our competitive edge by which we live and often perish in business. It has taken what was in the transition between agrarian and industrial where we came to common-gauge rail and power standards and you name it, but basically took a country of 50—at the time—states and started to meld into a nation so that we could compete in a global society in an industrial way.

My sense is this will be equally important in the 21st Century and clearly will be where our competitive edge is won or lost, and is likely to change our relationship on a more international scale, mostly because of the speed and the tremendous economic advantage that we get in each and every transaction that we undertake on these networks.

For the Department of Defense, this is in our mind and the way we handle it as a weapon system. It has to be. The discipline that we demand to operate in this environment, the standards that will be necessary to operate in this environment, we have to treat it as a weapon system. That carries with it a certain amount of responsibility. It also carries with it a certain invasiveness that we could not have in the private sector, and I'll talk a little bit more about that.

But this is not something that is a passing fancy. It is pervasive in our lives, in our industry, in the way we do business both in the public sector, in personal lives, and certainly as a government. It is by all definitions a critical, vital national interest. The only definition that it doesn't fit when we're talking about critical, vital national interest is the attention we're paying to it.

Now, you're the wrong group to say that to, but you know it. And so when a few years back somebody said, "Oh, you're going to be STRATCOM, and oh, by the way, we're going to give you cyber," and I had to go to the dictionary and do all those things, a smart Secretary of Defense said, "You might want to start with law." It actually was a pretty good piece of advice.

And so for us in the Department the construct that we work against, which is in law, has two dimensions principally. The first is that the Department of Defense generally picks up responsibility for those things once we leave the shoreline, and we build ourselves out to protect this homeland. And inside the homeland, only those things that are associated with our bases and our ability to get out of the country. In cyber networks, we generally talk about dot-mil being our responsibility, and we have authorities vested in us in law that allow us to work offshore with other partners and the government. Once we come onshore, it's the Department of Homeland Security, unless somebody invokes military support to civil authorities or insurrection if we got that far down the road.

The Department of Defense, because of its history and all of the activities around it, brings to this a scale that is pretty significant, and it needs to be worked on a global scale. And that's the good news. The number of people we have trained, our real expertise in this area, does not have the scale that we need. We're talking, and we just patted ourselves on the back because we're working through training a thousand new people a year. That's about a third of where we really need to be in this environment, but that's the scale that we're trying to work to. Imagine a service—you pick it, Marine Corps, Air Force—let's look at the first F16, F18 squadron you're going to shut down because you're going to convert those people to cyber. But those are the decisions that we're trying to work our way through.

The second dimension of this thing is the layering, and the construct that we are trying to put in place, which would fit with other constructs within the government, is at the core have your most protected, most resilient, most capable networks, and then work your way out. Because we're treating it as a weapon system, because we are the Department of Defense, there is a certain intrusiveness that we can have that the general government, the rest of the government and the civil sector cannot have. We can basically tell people, "Check your rights at the door. You're in the military, and everything you do has with it no expectation of privacy." That generally is a difficult sell in the public sector, to say the least.

But we can do things there that others can't, and then we can move out to dot-gov and we can start to work at dot-gov, and then out to dot-com. And that layering, along with what you can do—and you all know, there are other types of networks and other layers of society that we can put on this—but in general terms that layering gives us a resilience and an expectation of availability that would not be expected in many other sectors.

Probably the greatest flaw that we're trying to deal with in this really commercially architected domain that you can turn on and off, unlike space and water and air, is our critical infrastructures out there in the Wild, Wild West called dot-com. And there are technical solutions to that, but they bring with them an intrusiveness and an expectation that is different in privacy than what the commercial sector is used to, and we're going to have to reconcile the cost benefit and be convinced that the benefit outweighs the cost to start to move it.

It is not a technical issue. I mean, we'll make technical issues out of it, but really it's not a technical issue. This is a cultural issue, and what you don't want to have happen, at least from where I sit, is what people have called a Pearl Harbor event. But you don't want to have to go through a 9/11 to get the feeling that it's important enough that the cost benefit has moved in the right direction and you can now start to protect things that generally live out there in the dot-com domain.

That is something that is very important to us. We're going to have to work our way through it. Forums like this start to build the conviction and the understanding of the cost and the benefit and how that should be weighed. What technologies could be put in place and how we can protect that which made us great, our diversity and our protection of personal rights, against a greater good, a common good, and where do the two cross and how do you start to work that? Which is a lot about what your game hopefully is focused on.

So we have those two dimensions of activity. We layer on top of that one of the unique areas of this environment domain, one of creativity, innovation, et cetera. I'll go back again and kind of use the industrial construct. It took us 100 years to build the repeater rifle in the Industrial Age. It took us five years to invent and deploy a nuclear weapon. And now we're dealing in Moore's Law. Competitive advantage, patent laws, are generally based on 30 years' worth of value in a good idea, and you're rewarded for that kind of a cycle. That business cycle doesn't exist anymore. Most schools will tell you it's 30 months today in the industrial sector or in the business sector. For us and IED and the changes there are 30 days. Thirty days is our business cycle for IEDs.

For the most part what we see, and this is a generalization but it's still reasonably accurate, when we're dealing with viruses, worms, we're talking two weeks. That's the duty cycle. You field it, I come up with a fix, you come up with a new one. Two weeks. PPBS, business processes of the Department of Defense, are based on a five-year cycle. So we're trying to do this with a couple of our hands tied behind our back, but it is the reality of the world we're in. It is the reality of the world that the business sector lives in. The cost benefit in the business sector has certainly—if you live this day in and day out which most of you do, you cannot afford to be attacked and wait for a month for a patch. You can't give up that profit. It's just not realistic.

And so that starts to pull us into this dialogue, which rolls off people's lips probably a little too easily, about how we need to bring the private sector into this activity, hook it up with the government sector. That is true to an extent, and I'll push on that a little bit more.

A couple other things that they told me that I must make mention of here. Integration of defense. Let's call it reconnaissance and offense. The networks have essentially been built on a point-defense construct. The firewall, either in your Systat side of the house or at your desktop computer, is what you rely on for protection. Point defenses in history have never worked because you hit diminishing returns on your investment so quickly, and you can pour more and more money in for an increment of improvement that is not worth the cost. But that's the construct that we're living on here.

So how do we change that area to global? And global's where we have to be. And how do you move beyond a pure defensive construct for which I can attack you freely and you have no penalty or recourse against me? Boy, if I'm on the other side of this equation as the adversary, I'm loving this world because everything that you do to impose cost on me as an adversary, I can trump you easily because there's no penalty and no cost for me to attack you. And that's got to change.

Now, that's not to say that Justice isn't out there doing things, but we do not yet have a construct between which the law of war and basic criminal law match up. And so we've got to start to think about how we want to do that, how we build that into the architecture so that we understand—it's kind of the duck walking by—when somebody attacks you, you know whether it is a law enforcement problem or a law-of-war problem. And we don't have that construct really put together yet.

So if there are generally accepted three levels of activity here, there's the hacker, there is the industrial espionage, and then there is the nation state layer here. And there is today a huge distance between nation state and industrial, generally driven by investment. How much are you willing to spend on this thing?

If we were to say that hackers and industrial is law enforcement and then we're going to apply our military resources to the high-end nation state, that would allow us to understand then where our investments ought to be, who should be making those investments, what their responsibilities were, what the R&D centers ought to look like, et cetera. We have not yet come to that taxonomy, and I don't know that that's the right one, but we've got to do it. Otherwise, you have the Department of Defense trying to defend against hackers, you have Justice trying to defend against nation state-scale crimes, and we're all over the map. So at some point we've got to come to reconciliation on that. It's just essential in the way we do business.

When you start to work your way through some of these challenges, like that taxonomy, you quickly come to an understanding that if we have the defenders sitting over here, and let's just say God bless the defenders, but when I came into the business at STRATCOM, that's all anybody wanted to talk about was the next iteration of a firewall. And then over here was a different group with a monetary center and R&D that were the offensive side of the equation. And then there were these guys called "exploiters." They either were doing intelligence, or they were trying to figure out what was going on.

None of the three worked for or with each other. I don't even know that they knew each other existed. So this is kind of the dumb Marine in me, but basically we had the defensive, we had the guys going out and doing reconnaissance, and we had the offense. And the reconnaissance guys would come back knowing where the bad guys were and not tell the defense, not tell the offense. The offense would go out and start shooting and not tell the defense they were shooting. In money parlance, the offense would use the defense's money for their investment, and the defense would offset all of their costs against the offense, so that wasn't coherent. I had 19 direct reports in the Department of Defense as a combatant commander that thought they were in charge of cyber. Nineteen. And there wasn't a single shingle in the Pentagon that said "cyber" on it.

Those are some of the challenges. Trying to understand how to bring this into a construct without hand-jamming it into an industrial construct so that we take five years to field an application and a change to it requires another five just to get through the investment process. We've got to understand how we're going to move forward as a nation in this area.

My last piece here is a little bit about the public-private government side of this equation and why it's important. On the R&D side of the house here, as we move into this networked world where we have ways to touch intellectual property legally, in a global scale the Department of Defense this past year, we all high-fived because we got to 3 percent R&D. We were still outspent by Microsoft, Cisco and everybody else as individual companies.

We have what I will probably unfairly call an Eisenhower construct in that we have a set of national labs, and we think we have all of the intellectual capital in the world, so we're going to invent a cutting-edge technology. We're going to keep it a secret for 30 years so that nobody can catch up, and then we'll dole little pieces of it out to industry. That model went away in the '50s, but we're still trying to apply it here.

And so there is an R&D aspect here that has to be joint with the civil sector. That doesn't mean that the civil sector has to give up their competitive edge; in fact, that's just the opposite. If we ask that, that's for sure not going to happen. It also doesn't mean that there aren't any smart people in these national labs that could be mustered up and work on this problem. In fact, I would tell you based on what I see today in our meetings with industry, much of what we're doing is well ahead of where they are. Much of what they're doing is well ahead of where we are. We are not doing the same things. And so the belief that somehow we're just going to all jump in the pool together and this will work is not the right approach on this, either.

I might as well shoot at all the ducks while I've got them out here. A world-famous, world-class think tank just put out their report, and I'll just leave it at that. But we tend to pull groups together under bureaucratic protections—FOIA, things like that—which were never designed to protect competitive edge. Never designed to protect the intellectual property. We have to get outside of the box and find what is a relevant civil government-private sector government relationship here that allows the nation to stay competitive in the decision cycles that are the reality of this networked world. Allow the government to protect the commons so that you can flourish out there and develop competitive edge on a global scale. And find the interfaces between our nation and other nations, the private sector and the government, in a way that makes sense.

And we haven't found that yet. I'd like to stand up here and say I've got the answer. I don't have it yet. But what I am relatively sure of after a few years of doing this, that trying to hand-jam it into existing structures, existing boards, et cetera, is not going to work. They just don't have the construct that will allow us to do what we need as we move forward.

So if this group in particular wants to put energy towards something, that's in my mind where your expertise would be incredibly invaluable. And people are putting stuff all over the chalkboard on this right now, but not a lot of originality there. And I don't mean to shoot at people that are trying to move this forward, but trying to jam it into the current structure, the current communication structure, the current organizational constructs like FOIA, are not going to do it for us. They don't give us the leeway that we need to have the intellectual capital focused in sectors that are appropriate for private and appropriate for government. They haven't figured out that taxonomy yet. They are generally organized of like-minded people, and this environment is not like-minded people. Its strength is that it's not like-minded people. So if you get all the wire-heads or you get all of the processor guys or you get all of the policy wonks—those are all affectionate terms—you're not going to get where you want to be on this, I don't believe. We've got to figure out how we can be sufficiently inclusive and still get something done in a timely fashion at network speeds.

My last plea here, and then I'll open it up. Back to the original part, this is a vital national interest. It deserves the time, the intellectual capital and the investment that that means, just like energy and numerous other things that we have declared as vital national interests. If we don't compete in this environment, we will perish in this environment. It's that powerful.

Thank you, and I'm happy again like I said to go in any direction you want to go, as long as I can see you.

Sir?

Speaker

Because of the cyber issue, modern warfare has forever changed. We will never go to war again without some type of a cyber component to it. How is the Pentagon dealing with that, and what is the way forward for here, whether it's professional development, career path? In a sense cyber is as important as the air war, the ground war. There would be also a cyber component. That's one.

The second question is you aptly described that this is very much an asymmetric threat where you can have an individual carry out a cyber attack and there's very little repercussions to that. Can you give some thoughts as to how we deal with the penalty? What type of penalty can be imposed so that we level the playing field and it's not just asymmetrical?

And then the third question is a bit maybe outside [your lane], but a lot of the things you talked about, how do we get the public in a sense to realize that there is a greater benefit to imposing some security than the current situation? How do we get the public to buy in? Since that's more some of the things that I deal with, I'm very curious to know just thinking outside the box, how do we get the public—raising awareness, how do we get the public more to buy into this?

General Cartwright

Let me start at the back end and then go forward because I'll probably forget the first part. But the public side of this equation and how we start to bring them on board, I think there's two dimensions to this, and it really applies then to your second question about how the services are thinking about this also. And so I'll start it with kind of talking about the services.

If we had this conversation a year ago, I did something that was controversial, and I'll take the blame for it. When we said that we're getting attacked on a regular basis on our networks and it was starting to degrade our networks on the unclassified side, and so we said we're going to have to take a look at Facebook and YouTube and some of these things that are eating up the bandwidth and also carrying some viruses along.

Those that were wearing stars, "Sure. Why not?" The human cry that went up from 35 years of age and down was reflective of our lack of understanding of how much they are connected to that lifestyle, not only in their social side but in their tactical side [inaudible 31:34]. So there is a broader—I hate to say this, but I believe there's a broader gap between those who wear stars on their lapels and those who have just a couple of chevrons than ever before in the understanding of this environment and the opportunities in this environment and the risks-benefit trades.

And I'll take a tactical example. The Secretary and I were down in Georgia, looking at the Army's future combat system for the soldier and talking to some young enlisted that were going through this training. And the quote that will resonate with me forever in the difference between how I probably think about

the battlefield and how they think about the battlefield: "I'd just as soon leave my M16 in the barracks than go without this stuff, this situation awareness."

That translates to the civil sector. The question is, when will that generation start to come? Because they have a very different calculus about intrusiveness into their environment, their willingness to share, their openness in these networks and how they treat them and how important they are to their lives. My worry is that we'll have to wait for generational change to really start to get at this issue and the willingness to make cost-benefit trades that will allow us to be in the right place, and that's not good.

So business probably is the leveler because you will perish in business if you don't understand this environment. That is not yet true in the military. And so I would say the private sector in this area is ahead of us, that we probably can start to have a dialogue and they understand just from the simple things of identity, loss, just day in and day out protection of what they would call the things they want to keep private versus what they want to share, and how they do it. They're probably going to be more tolerant of things that protect their opportunity and give them that opportunity than we are—I'll use myself—certainly at this age group.

So that to me in both your second and third questions is a little bit of how we do it. I think the first one was what are we doing from a standpoint of tactical? How do we think about this, and how do we start to train towards it?

The training can't come fast enough. The interesting thing for me, we're just working our way through and putting the finishing touches on an activity that would say that what in the past was the bandwidth that you would give to a corps, we're just finishing up making sure that gets down to the company level. This nation, the world, in 2006 created what are called 40 exabytes of unique information. What's an exabyte? Three hundred thousand Libraries of Congress. Today, we're storing at the edge out there in places like Kandahar and Bagram and Fallujah, we're storing in probably about a 30-day period several hundred terabytes, and we're keeping 90 days' worth of activity at the edge with programmers. That's the way we do business. That's the only way to stay inside of the decision cycle.

And a commander that doesn't know that is irrelevant. He's irrelevant or she's irrelevant that quick because she can't lead or he can't lead because the people they're trying to lead, that's the way they think. That's what they need. They need those decision cycles, those transaction rates, the scale of that and the processing power and storage, not back in Chicago. They need it in Bagram.

And if we don't understand that, they don't have tools. We build today—pick it—the Marine expeditionary fighting vehicle, the F22, you pick it. We know exactly who that's for. The problems they're trying to solve are the problems that we hadn't anticipated that we only have two weeks between life and death. Those will only work and you can only lead when you understand how to stay inside those decision cycles and deliver capability to soldiers, sailors, airmen and Marines out on the edge. And business will not be far behind us on that.

So to me, what we're challenging are senior captains, colonels, generals, to understand is if you want to stay relevant, if you want to lead in this environment, you have to understand it. You have to be able to fight in it. You have to be able to think in it. You have to be able to lead. And if you can't, the only one that won't know is you. And that's how I generally try to wake them up in the morning when I talk to them. Because you will be irrelevant in this environment so quick if you don't try to keep up. You

cannot lead. You cannot wear rank and be credible if you do not understand how to fight in this environment.

The other piece, and you've allowed me to get on a soapbox so I apologize, but the other piece that is so important for military from my perspective to be able to lead in this environment is to understand—and people often say, "Okay"—and I did the same to you—"Cyber, how are you going to defend in cyber? How are you going to do offense in cyber? If somebody attacks you in cyber, how are you going to go back?" And the first thing you think about is, "Well, I'm going to do some cyber offensive tool. I'm going to go attack them in cyber." No good commander understanding the art of war would ever attack on the same vector they were attacked on. You can't.

So you have to have these other tools. Why would you cede surprise and knowledge to your adversary? So you don't deter cyber in cyber. You do have things that are tools in cyber that you use for deterrents, but if a country attacks us in cyber, at least from this average Marine, I'm not coming back at them in cyber. I'm going to make them pay, and no matter what they do to me, the end is not going to be any different. Trust me. And they should have no doubt about that. We're not going to cede that.

So kind of long winded. You let me get on my soapbox here, but these are things that are really important to understand from a leadership standpoint and how we bring up our officers and our senior enlisted in this environment. And if they think that three schools between the time you go through boot camp and the time you are a four-star general are going to keep you on the cutting edge and keep you relevant as a leader, you are sorely mistaken. It is just not the case. Just not the case. This is a very, very dynamic environment.

Sir?

Speaker

[inaudible 39:30] if you're attacked. If you have a cyber attack in DOD on the Pentagon, I was going to ask you, how do you decide whether it warrants just defensive actions, or how does it warrant offensive actions? You've just said that you wouldn't respond to a cyber attack with a cyber attack. I find that surprising. Would you not try and neutralize something that's coming at you with a cyber response?

General Cartwright

I'm certainly not going to go into the classified side of all of the tools that we have, et cetera. But the layering that I talked about gives us a resilience that may change the speed of advance. It's like working with armor. I can afford to go fast if I know what's in front of me and I have high confidence that I know what's in front of me. Throw some ambiguity in, and I'd like a little bit heavier armor. I'll move a little slower. I'll probe, et cetera. But it's not that different in cyber.

The law of armed conflict still applies, so that's pretty straightforward. And so if that cyber attack, even though it may have been meant for the Pentagon but it knocks out the FAA or it gets at a hospital or all of the other criteria associated with the law of armed conflict, then it is the law of armed conflict. The hard part about this environment is attribution and understanding attribution, and you can get it to an extent, but it is not exquisite. It is not good enough to put a Social Security number on it or cross-hairs on a forehead yet.

And that's why you want to look in other venues. We don't now have probably as robust as we would—in fact, we don't—policies, declaratory policies, declaratory policies that match up to law, that match up

to treaties, et cetera. And they may not be the right construct, but we've got to have that bridge that takes you from law to policy to actions, and it has to be coherent so that PFC Cartwright, when it goes by, knows exactly what's appropriate, what's proportional and how to handle it. And whether he chooses to respond in cyber or with an M16, he knows what is appropriate and how to handle it, and then the art of war should kick in. Because what you want to do is just change the calculus in your enemy's mind in an appropriate way that is proportional to the threat that you just received.

So to me, one, if you're going to take cyber away from me, if you think you're going to take my networks away from me, it ain't going to change the output of the equation. Sorry, that's Marine talk. It just isn't going to change. You're going to lose. There shouldn't be any doubt in your mind you're still going to lose. I don't care what country you are, you're going to lose.

Second, don't expect me to come at you the same way you came at me. That's just art.

Third, these networks are more resilient than anything we ever had in the past, not less. And that's something that gets lost in these conversations about information assurance, often. These networks are leveraging. They have a huge and incredible resilience compared to the circuit-based activities we used to deal with. Anybody that's ever been in the service, anybody that's ever been in business, in the service after every exercise and every conflict, the [CALM 42:52] in the intelligence sucked. The CALM is not on that list anymore. It just isn't. The passing of information is not on that list in the Department of Defense anymore. You don't hear it in an exercise. You hear about things you'd like to have had, but they are, "Jeez, I wish I'd had about twice the bandwidth," type discussions, not the zero discussion.

These networks are very resilient. You bet there are vulnerabilities. But there is nothing that I've ever dealt with that doesn't have vulnerabilities. That's why they put you out on the battlefield. If it were perfect, we wouldn't have to go out there.

So that's kind of my response to what happens when the Department of Defense, the Pentagon, whatever, gets attacked. Did it break the law of armed conflict threshold in law? If not, then what's appropriate there? And that's generally going to tell you that you need to tighten up your defenses, if it really matters, if it was significant. Look at the policies. Are they appropriate? Have they allowed you to do the right things? And what's your resilience to continue on, should the escalation occur? How do you stop the escalation? And probably, particularly in the private sector, how do you control the escalation? Is generally the tactics that we're trying to understand on a given day.

Sir?

Speaker

So General, a quick story and then a plea. The story is I was doing the terrorism portfolio at the White House during the last transition, and when the new team came in, they thought they understood the terrorism threat. But two things they didn't understand. They didn't understand the magnitude or the urgency. And they as much as anyone else in Washington were unwilling to elevate that issue on the foreign policy national security agenda at the expense of other issues.

So let's fast forward eight years. We have a new team coming in who may think they know the issue but don't understand the magnitude nor the urgency because they've been on the outside for the past eight years. Nor are they willing—hopefully that's not the case, but maybe—not to elevate this issue at

the expense of other issues because in effect the agenda's got even more complicated than it was eight years ago.

There has been a tremendous amount of work done in various pockets around Washington in the past few years, most of it done by the DNI in raising awareness and getting people bought in, but it's still pockets. Washington is still a town that deals with kinetic threats and kinetic responses.

So the plea I have is you, the Chairman and the Secretary are uniquely positioned to educate the new team on why this is a national security issue and an economic security issue, and that if you go in and do that, then I feel pretty confident we will eliminate some of the mistakes we made eight years ago when there was an opportunity for folks and that opportunity was missed. That overdramatizes a little bit, but if we're truly serious about this issue and we understand the magnitude of where it might go, then there is an urgency to act. And you, the Chairman and the Secretary have a tremendous opportunity to do something about it.

General Cartwright

Was there a question?

Speaker

No, that was a plea.

General Cartwright

Sorry. No disagreement. I mean, I'm not passing judgment on transitions in the past or now or in the future. But when I had an opportunity to bring this conversation to that level, the good news was once we got through the understanding of kind of the technical side, it was easy. But it only took about 30 seconds to understand the vital national interest side of the equation. It's too pervasive. Even if you are not 35 and below, it is too quick.

And so the import I don't worry as much about. Our larger challenge, and you alluded to it and I'm going to more personalize this inside the Department than outside, but when are you going to be willing to give up an F16 squadron for this? The institution is heavily biased towards kinetic, material, et cetera.

Now, you happen to have four service chiefs right now that are completely captured by the import of this activity. There is no doubt in their mind that they have to make major service cultural adjustments to start to address this. But it is still very much an industrial mindset that runs the bureaucracy, and it will compete, as you say, with boutique issues of the day, whatever they happen to be. That will still be an activity we have to work our way through. But people are voting with money. They're voting with intellectual capital. They're voting with risk to step outside the box inside of services and inside of combatant commands today in ways that two years ago it just wasn't there.

So I have hope. My glass is half full, and I certainly have hope with the next administration. I think that is understood. It is the technical and policy and how do you do it, how do we start to build the capstone policies that then allow us to judge all of the underlying law and policy in the nation to make sure that it advantages us? And how do we step out of the national construct into the international construct because a national construct is not good enough? I think we'll learn that very quickly.

So it's a great statement. It will be the challenge. I'll certainly do my best.

Thank you.