THE BROOKINGS INSTITUTION

FALK AUDITORIUM

INVESTING IN THE FUTURE OF U.S. DEFENSE DURING A TIME OF TRANSITION AT HOME AND ABROAD

Washington, D.C.

Monday, December 5, 2016

PARTICIPANTS:

Moderator:

MICHAEL O'HANLON
Senior Fellow and Co-Director, Center on 21st Century Security and Intelligence
The Brookings Institution

Featured Speaker:

ROBERT O. WORK
Deputy Secretary of Defense
U.S. Department of Defense

Panel:

ALAN EASTERLING
Corporate Director, Strategic Development
Northrop Grumman

WILLIAM LYNN
Chief Executive Officer
Leonardo North America and DRS Technologies, Inc.

KELLY MARCHESE
Principal
Deloitte Consulting LLP

* * * * *

P R O C E E D I N G S

MR. O'HANLON: Well, good afternoon, everyone. Welcome to Brookings. I'm Michael O'Hanlon with the Foreign Policy Program, and I have the real distinct honor of hosting Deputy Secretary of Defense, Robert Work, today. Very glad to have all of you here as well.

We will have a discussion up here, the two of us, for a while, then involve you in some questions, and after that part one has ended and Secretary has departed, then we'll bring up the panel to discuss more about the topic of today, which is, as all of you know, innovation in DOD, but specifically, the issue of the third offset, and many other concepts and issues and programs that surround it.

And we'll get into anything else, and we'll go in different directions, as well, but that's where I want to begin anyway. And I'd like to first after I give a couple more words of introduction ask you to join me in welcoming the Secretary.

But first, I think many of you know him already. He's a 27-year veteran of the U.S. Marine Corps, and distinguish service around the world, including in Japan and elsewhere in that period of time.

He, as I've said earlier, and as you all know, the Deputy Secretary of Defense, a job he's held now for about two-and-a-half years. He along with General Dunford and others, but especially, I think, Secretary Work, is really the father of this concept of the third offset, which we'll discussion in just a moment.

He was Under-Secretary of the Navy. He was at SCBA thinking about long-term trends in warfare, the Center for Strategic and Budgetary Assessments that as you all know is at the forefront of thinking about these kinds of questions, and he was also the leader at CNAS for about a year prior to rejoining the Pentagon in 2014.

So please join me in welcoming Secretary Robert Work to Brookings.

(Applause)

And Mr. Deputy Secretary, thank you for being here. I would like to begin by really just asking you to, even though most people in this room have read you on this topic before, heard you on this topic before, since we are in December of 2016, and it's an important moment to hear a distillation of how you would just define the concept of the third offset.

SECRETARY WORK: Well, first of all, Michael, thank you for having me over. It's a pleasure to be here, and hello to everyone.

If you think about this, the third offset is nothing more than trying to maintain what we would call our conventional overmatch to the greatest extent possible. And our feeling is if we can do that, we will strengthen conventional deterrents and make it less likely that we will ever have a collision against a large state power.

Now, I think all Americans know, I mean, over the last 15 years, counter-terrorism, regular warfare, counter-insurgency, nation building, those are messy, messy jobs. They aren't something that happen fast.

But I think the American people believe that at least in terms of conventional warfare that generally we have short, sharp, victorious wars. They go back to Desert Storm. The go to Operation Allied Force in Yugoslavia. They go to the initial conventional campaign in Iraq. And they say, wow, we have this conventional advantage. And that's true against small, regional powers, but it's not true at all against large state powers.

And so all the third offset is, is how do we make sure that our conventional advantages are so evident and strong that it would deter a conventional conflict with a large state power? And so that's really what it is about.

Now, Michael, if I could, please, it takes place within a framework of comprehensive strategic stability. And any of these frameworks that professionals, they can be very easy to understand, but this is the way I think of it.

You have strategic deterrents. You have to get that right against large state nuclear powers. Got to have that. You've got to have at least strategic parity. You've got to make sure that it's nice and stable, and from our perspective we include nuclear weapons in that. We include strategic cyber, cyber that would be used against the infrastructure of a competitor, and tactical nuclear weapons.

Then there is conventional deterrents. And that is trying to forestall any type of a conventional conflict against nuclear and great powers because that would disastrous if we had something like that.

And then it's managing the strategic competition on a day-to-day basis, making sure that it doesn't get too hot. And I think the connection between managing the competition and conventional deterrents is crisis management, and the connection between conventional deterrents and strategic deterrents is escalation control.

So the third offset is not a unified field theory. It focuses only on strengthening conventional deterrents within that framework, and that's what it's all about. It's nothing more than making sure, trying to make sure that we don't ever have a conventional war against a great power.

MR. O'HANLON: Thank you. So I want to do a couple more things in regard to this concept, if I could. And one is to begin with a little bit of an historical perspective.

As I think I've told you before, I'm a fan of the term, "third offset," but it requires one to have some sense perhaps of what the first offset and the second offset

were, and that's part of why some people don't love it as much as I do because they don't want to have teach a history lesson.

SECRETARY WORK: You and I are the only ones who like third offset, Michael.

MR. O'HANLON: I think there are a few more. And, actually, I do want to, in a minute, I'm going to ask you how it relates to all the other panoply of concepts that we've heard from DOD over the years, different kinds of initiatives, and how you would say it either builds on them, supplants them, combines them, what have you.

But first, I want to do a little bit of a take, ask you for your perspective on the first and the second offsets. Of course, and some people even define these slightly differently, I would define the first offset as essentially the full range of nuclear capabilities that we built up in the early years of the Cold War, but some people will really emphasize the tactical nukes, and the geographic dispersion of nukes.

Some of that I didn't really like in retrospect because it involved things like the pentomic division which got our Army thinking about using battlefield artillery in the form of nuclear weapons, so I'm not sure every aspect of the first offset was equally successful. We'd love your comment on that.

But also on the second offset which I think was more of wholesale success, the notion of using precision and largely coupled with air/land battle the doctrine of NATO in the late seventies and eighties.

So I would just love to hear your quick take on those two previous offsets. How well did each one of them work. Do they offer lessons for today?

SECRETARY WORK: Thanks, Michael. Look, any offset strategy, and that term was coined by Paul Kaminsky and Bill Perry when they were describing what they were trying to do in the 1970s, which was known as the second offset.

And so there's a couple of things that are always in an offset strategy. First, there are technological advancements that help the strategy along. But they're really focused on operational and organizational constructs that are designed to provide an advantage at the operational level of war, which is the campaign level, the theater level, the combatant commander level. Think General Schwartzkopf.

So that's what makes an offset strategy. And so the first offset strategy can be tied directly to President Eisenhower's new look strategic, and it was based on the premise that we had strategic nuclear superiority, but we were outnumbered to a great degree in Europe by the Warsaw Pact.

When he came in as president, he asked his military planners how many NATO divisions would it take for us to conventionally deter Russia, and the answer came back 92 divisions. And he said that just doesn't work for me. I'm not going to spend that much money to have that big of a forestructure. Even if 28, even if every single NATO country provided one division, it would still be an awful lot of money.

So he said we're going to exploit our nuclear superiority and rely upon battlefield nuclear weapons for conventional deterrence.

And, Michael, as you say, you can look back in the fifties and just scratch your head and say, wow, this was kind of la-la land. But it worked. And the reason I (inaudible) debate with Joe Nye, there is a lot of, there is an argument that the first offset didn't work. But the way I believe it did work is Soviet operational art, which was to attack NATO in these successive echelons of heavy forces, create a breakthrough for a thing

they called the operational maneuver group that would go deep into NATO's rear. That was specifically designed to prevent NATO leaders from using tactical nuclear weapons.

So did the first offset work? It sure did. It convinced the Soviets that they needed to change their operational art. And they did.

Now, in the 1970s what happened is the Soviet Union gained strategic nuclear parity. And so the threat of using tactical nuclear weapons on the battlefield and risking an escalation up the ladder just wasn't credible anymore.

So what was the choice? And we had a long-range research and development training program, and the first choice was to make nukes usable. Neutron bombs. Smaller nuclear weapons. Dialable yields. And that didn't sound too attractive to our national leadership either because of the risk of nuclear escalation.

So they said we're going to go after conventional weapons with near zero miss. That was the way they described it. We all know them today as precision-guided weapons.

And it was the battle networks that would employ them. Being able to look throughout the theater, see where Soviet concentrations were, it was called Look Deep, Shot Deep, and you would be able to apply conventional weapons against them. That was the second offset.

So now, just like what happened when the Soviet Union achieved strategic nuclear parity, we had to change our first offset. Now, Russia and China have achieved rough parity in battle network and guided munitions warfare, and the United States military has never faced an adversary that has battle networks that are as, can see as deep as ours, and can shoot guided munitions in the density and numbers that we can.

So, therefore, we have to think of a third offset. So I agree. I mean, I like the historical progression of this, and we can argue over, you know, there were all sorts of things that, jointness was important in the second offset. The all volunteer force was in the second offset, but the operational level of war was having these battle networks that we demonstrated in Desert Storm with conventional guided munitions that really changed the game. And the Soviets knew it.

In 1994, General Ogarkov, who was the head of the Soviet General Staff said, my goodness, the Americans can provide the same destructive effects with conventional munitions now that they threatened to do with tactical nukes, and it was a big game charger for us.

MR. O'HANLON: So that's a great -- I'm glad you mentioned General Ogarkov at the end because that sets up the progression of where we've gone since that time because, of course, I think it was that general who coined the phrase, "military technical revolution."

And so you just, this is very useful. You sort of capture within the second offset the movement to the U.S. all volunteer force, and you've mentioned jointness hitting at Goldwater/Nichols, perhaps. So if we take that mid-1980s period as sort of the combination of the second offset, after Desert Storm, we saw a lot of terms introduced into the lexicon, and some of them were associated with big Pentagon initiatives as well.

So we talked about revolution in military affairs. That was a big dreamy concept, but then it got translated into military transformation as a guiding concept within the Department of Defense.

And then we've heard other terms, as well, in recent years. We've heard full spectrum dominance. There's always a joint vision 2020, or 2030, or 2040. There's

air/sea battle now reamed joint concept for access and maneuver in the global commons. I said that all with one breath.

SECRETARY WORK: And you remembered it. (Laughter).

MR. O'HANLON: And so, you know, there are other things cooking as well, more specifically in regard to missile defense or undersea robotics, or what have you.

So you've defined third offset very crisply earlier, but now I wanted to ask how does it relate to these other things that I just mentioned? Does it encompass them all? Does it sort of, should it be seen as sort of a latter Obama administration's effort to keep all those things going, or does it have a new sense of prioritization within those different sub domains?

SECRETARY WORK: Well, without question, the Soviet general staff understood what happened if you put together these battle networks at the campaign level, and you employed guided munitions throughout the breath and depth of the battlefield. They got it in 1984. I would argue that we didn't, we, the United States, didn't get it until Desert Storm.

Now, the ironic part of Desert Storm is only 8 percent or so of all the weapons dropped in Desert Storm were guided. Almost all of them were unguided bombs. But I'm old enough to remember, and I see some of you are in this room, I hope you don't think this is an insult, you're old enough to remember too, General Schwartkopf every night saying, boy, this is one lucky Iraqi vehicle and it's cross a bridge. And as it crosses the bridge, right behind it a bomb hits right in the center of the bridge and collapses it.

And so that really triggered everybody's understanding of, whoa, this truly is different. And then by Operation Allied Force, 50, 60, 70 percent of every shot we took was a guided munition.

So military technical revolution was the Soviet term. Andrew Marshall and the Office of Med Assessment did not, what he said is this is all about operational and organizational constructs. It's not about the technology per se. Technology enables it. So he used the term, "revolution in military affairs."

That was just a difference. He said it's a revolution in (inaudible), a revolution in concepts. It's a revolution in organizations. So military technical revolution and RMA I would say are the same.

Transformation then became the term of the Bush administration, Rumsfeld, the Rumsfeld secretariat, in which you would take these ideas and truly transform.

Up through about 2001, the argument was, hey, this is all about the number of guided emissions you drop. But let's change the force. Let's have new operational and organizational constructs. And if you look at the 2001 QDR, we would have headed that way had 911 not occurred.

So the third offset really says here's the difference. Now for the last 25 years we haven't had to worry about great power competitors. Now we do. Both China and Russia I would define as a great power. Both of them have achieved parity with us, and so we need to make sure that conventional deterrents are solid.

So I would say along the sweep of history it's a continuation, and it's just a little bit of a different focus. The Chairman of the Joint Chiefs talks about maintaining a competitive advantage. That's when he talks about it. That's what he talks about.

When Secretary Carter talks about it, it's about being innovative, and being at the cutting edge. So it's all part and parcel of what the United States has tried to do in its military strategy, and that is to avoid a war with great powers not to fight them.

MR. O'HANLON: So now let me, if I could, and again, just taking sort of different slices at the same big issue of, a big subject, I want to ask you about a few areas of technology. I'll just lump them together and ask for you to comment on which ones you see as perhaps the most important within the third offset.

I know some of your background is in biology, but also space, and so those are certainly two big areas, right? So everything from enhanced exoskeleton kind of concepts, other things that help the human being operate more effectively on the battlefield to our use of military space, and the way that's evolved into really a critical part of our tactical war fighting. Whereas, in the days of the first and even the second offset, it was really much more about facilitating a strategic nuclear mission as opposed to the tactical mission.

And so we have space. We have biology. I've heard you and General Selva talk about artificial intelligence, and, of course, that raises the broader subject of cyber.

And then there's the issue of robotics. And some people would mention additive manufacturing 3-D printing. You know, again, some of these technologies overlap with each other. I'm not suggesting this is a list of sort of mutually distinct entities, but these are some of the big areas.

And then, of course, there's missile defense, which combines many of the other concepts, and may or may not make use of directed energy as a future enabling construct.

So if I put those things on the table, AI, robotics, cyber and related issues, space, enhanced biological weapons, or enhanced biological mechanisms to improve human performance, missile defense, directed energy, are there some of those that you would prioritize as being even more important than others within the third offset?

SECRETARY WORK: Sure. It's a great question, Michael. Well, let me start this way. Third offset, we don't know the destination of the third offset strategy. We kind of knew what the offset, the destination of the second offset and the first offset strategies were because we had a single competitor, and we could pick where we dominated them and the competition, and we said we're going to ride this train and we know if we get it right we're going to have a competitive advantage.

We don't have that today. We have two great power competitors. Many of the capabilities they're developing are similar, but some are different, and you have to approach managing the strategic competition with them in different ways.

So, we know that we have an advantage in jointness. Both the Chinese and the Russian military planners would like to gain a level of jointness. We know we have, we believe we have a competitive advantage in people. We can talk about that more if you want, Michael.

We have a big competitive advantage in being able to put together these operational battle networks, these campaigns. We've been doing it since 1990, and we do it better than anybody in the world. And we have allies which our two big large state competitors don't.

So we said the first thing we'll do, we don't know exactly where we'll head. Biomedics, genomics and biosciences might out to be even bigger than the way we're thinking now. But what we want to do first is make sure that our battle networks improve dramatically.

Now battle network it's very simply to understand. Think of the British home air defense network in World War II. There's a sensor grid. So they had radar. They had spotters with binoculars. They had electronic warfare guys. And that would tell them what was happening in the environment.

Then you had a command control communications, at that time, they didn't, but today we have computers and intelligence network. So they had underground fighter command centers that were connected by cable and radio. They had the distributed centers, et cetera.

Okay, this is what's happening. This is what I want to do. And then they had an effects grid, and the effects grid included Spitfire and Hurricane fighters, radar controlled anti-aircraft, barrage balloons, all of those things. And then they had a maintenance grid.

So we said how will we improve our battle network, and we asked the Defense Science Board what's the best way to go about this, and they said there's one competition you must dominate. This is the key competition. Artificial intelligence and autonomy. Putting artificial intelligence and autonomy into your battle network in a way that is consistent with your strategic culture is the most important thing you can do first.

So, actually, we have five things: burning machines, human machine collaboration, which is just using computers to help humans make better decisions; assisted human operations like exoskeletons, wearable electronics, wearable decoys; man/ machine, man and unmanned combat teaming, just, you know, robots and people working together; and then better autonomous weapons. Those are the five areas we're going to start first. The exoskeleton would fit right underneath assisted human operations. AI and autonomy is those five things spread broadly through each of the grids. Missile defense is an autonomous weapons and effects grid, and allows you to

dominate a salvo competition. They are shooting a lot of missiles at you. We're shooting a lot of missiles at them. You want to be able to knock down their salvo. Robotics are part and parcel with manned and unmanned system.

So everything you've mentioned with the exception of biology is totally consistent with the third offset. And an important distinction, Michael, we call it assisted human ops. In other words, we're empowering the human.

Enhanced human operations, I can easily see our state competitors going in that direction and saying we want to genetically modify our soldiers so that they can go 48 hours without sleep. That's scary to us. You know, that's not something that we are pursuing. We think of it in terms of assisted human ops. So everything that you said with the possible exception of biology is right in the third offset.

MR. O'HANLON: One thing that occurs to me coming off that is the possibility of machines deciding when to shoot. And I know this is going to be a long, hard problem for the rest of our lives and beyond, but do you have any guidance that you feel like you are able to at least help this decision-making along to the next step that has come out of the third offset or your work as deputy secretary?

SECRETARY WORK: Sure. This is very, very simple. I mean, I can't tell you how many times I get asked about Skynet and Terminators. In fact, Paul Selva, my battle buddy, Vice Chairman of the Joint Chiefs, he calls it the Terminator conundrum.

Well, this is what I can tell you for certain. Authoritarian regimes may gravitate towards more delegation to machines. Why do I say this? Because the Soviet conception of the reconnaissance strike complex was totally automatic.

We developed our battle networks totally different. We went to chat rooms. Everyone connected throughout the battle network. If an 18 pilot coming off missions saying, hey, we saw this. We didn't expect it. This is what we tried. It didn't

work. Try this when you go up. There's chat rooms throughout -- our conception to battle network is empowering human decision-makers. Whereas, an authoritarian regime might go to a totally automated system.

Now, the only place that we can conceive of delegating authority to a machine is in those cases where machine speed is critical. A cyber attack. If you don't have learning machines, smart machines fighting back at the very instant of the first cyber attack, you're at a disadvantage, and you'll probably lose over time.

Electronic warfare, same thing. So we have ideas of cognitive electronic warfare. And in missile defense, since 1986, the United States Navy has had an automatic option in their Aegis Combat System. So if there are 60 missiles coming in, remember all of the World War II missiles where the guys in the CIC and they're writing on the glass backwards, and they're saying, okay, the airplanes are coming in.

Well, you can't do that when you have 60 missiles screaming in at you at Mach 2 or 3. So you hit the I believe button, but it's a very prescribed defensive operations. In every case where there's an offensive decision to engage lethally, a human will make the decision, and the machine will simply execute what it's gold to do.

MR. O'HANLON: Thank you. As you look over the last two-and-a-half years particularly, but, you know, the whole Obama legacy and, frankly, even before that, do you see technologies that you feel have come the furthest and have now allowed you and, by the way, I hope you stay on past January 20th and there'd be a kind wish form the point of view of you and your family, but, and I don't know the prospects. I won't ask you to comment.

But as we are at a turning point, you know, the president is going to change no matter what, and the Secretary of Defense it would appear, and so what can

we take stock of at this moment. What have we really been able to see progress substantially? What are some of the accomplishments you're most proud of?

And the next question which will be my last question is going to be which programs do you most hope that, you know, the next administration will sustain or build upon? But taking stock and looking back, where do you think we've made the greatest progress?

SECRETARY WORK: Well, the third offset is very much like revolution and war theorists look back in history and they say, hey, this was a revolution in war. And the one that I think about is the rifle, telegraph, and railroad revolution.

It was a revolution that was driven by commercial technology. I mean, the telegraph and the railroad was being driven by commercial interests to, you know, provide rapid transportation of goods and people. You know, having more instantaneous information.

And whenever you have something that changes society, it will inevitably change the way you fight wars. The same thing's happening with AI and autonomy in our lives. I mean, just think about the last ten years. We're now, you know, we have autonomous breaking systems which take over from the driver.

I mean, it doesn't matter if the driver is talking to their wives, or their spouses, or they're talking on the phone. It doesn't matter. We have a system that says, hey, dummy, you're about ready to hit something that's not moving, and looks pretty big. We will stop the car for you.

And that's happening now. We have smart thermostats. We have smart refrigerators. We have Echo, you know. Hey, Echo, what's going on? That's changing our society. It's going to change war.

And I believe now everyone understands that really understanding how learning machines work, and how we collaborate with unmanned systems, and how we do human machine collaboration where the human is central, I believe that is the most biggest advance that I've seen.

And you can see right now in all of the services all sorts of unmanned and manned combat teaming and new instructions.

The thing I'm most proud about is really two-and-a-half years ago when we came, or when we started thinking about this, both of the first two offset strategies were driven from the top down. It really was the president in the first offset strategy, and it was Bill Perry and Harold Brown in the second. They were saying, look, we know we're comfortable in this way. This is the way we have to go.

So Secretary Carter, and I believe very strongly that we needed, and Secretary Hegel, we all kind of agreed the same thing, (inaudible) kind of top down driven and said we have to think differently in the future. Conventional deterrence is too important to assume that you're going to have it.

So I think the thing I'm most proud about, Michael, is not any technology. It is the fact that I really do believe things like multiple domain battle in the Army, all of the things that Admiral Swift is doing in the 7th Fleet in terms of their integrated battle networks. The fact that the Army is setting up its first tactical cyber electronic warfare unit. The fact that we now have a JIGSPOC, the Joint Interagency Combined Space Operations Center which is designed to fight our space constellation if it's come under attack.

It's the operational and organizational constructs that I'm most proud about, and that's why I'm relatively optimistic that this will continue whether it's called third offset or whatever it might be.

MR. O'HANLON: So great. And then that leads to my last question, and then we'll go to all of yours. I think we've got 15 or 20 minutes with discussion. But in terms of -- and David Ignatius, I know, got at some of this last week in his article based on your thinking, but if we look at the future, are there certain areas within the budget, within the broader DOD space certain program that really need a shot in the arm, or that might be seen as vulnerable by some, but really need to be sustained, any kind of particular guidance just as President Obama, as President-Elect Trump to think about keeping the coverage options within Obama Care even if he was going to dismantle some of the rest, sort of the equivalent here within DOD, do you see any areas that people may not fully appreciate the importance of what's going on, but you feel that it's really crucial to sustain the effort or even build upon it.

And you could answer at the level of the overall R&D budget, or you can talk more specifically about certain technologies as you wish.

SECRETARY WORK: Sure. The Secretary likes to say, look, we spend about $70 billion a year on R&D, and to put that in perspective, that's twice Google, Apple, and one other company combined. So we spend a lot on R&D.

The third offset is really about getting towards these new operational and organizational constructs. And so what we've done in the last two-and-a-half year is do a lot of seeding of demonstrations so that the next administration, once they know what their top line will be, they'll be able to pull however many levers they want.

So we have advances in aeronautics, advances in hypersonics, advances in unmanned systems, advances in new autonomous weapons, advances in learning machines, and we don't have the tails in our budget to sustain them.

We've purposely done it this way because Secretary Carter said, look, in 18 months what we've got to do is provide a basis for the next administration to be able to say these are the priorities we want.

So rather than give you a specific example, I would say that I believe the incoming team will be very pleased with the range of options that they have to choose from, and then the options that they choose will reveal their priorities and say this is what they think is important.

MR. O'HANLON: Great. Excellent. Well, let's go to you. Please wait for a microphone after I call on you, and please make sure to give your name before posing a question to Secretary Work. We'll start here.

MR. BERTUKA: Hi, Mr. Work, Tony Bertuka. Secretary of Defense.

There seems to be a lot of renewed focus now on the size of the force. We see that in the NDAA. Lots of money to stop the drawdowns of the troops. We see the 350 ship Navy proposal from the incoming administration.

This is an old debate about capability versus size. But as the debate seemed to have reemerged, what is your hope for the progression of it, especially in a resource constrained environment, size versus capability, and the third offset, it doesn't really put ITS emphasis on size, on a 350-ship Navy. You know, what are your hopes for this?

SECRETARY WORK: Well, IN an ideal world, and with defense budgets, pretty healthy defense budgets, hopefully, we would be able to do both capability and capacity and go after it.

But I'll just give you one example to the challenges that we face. In the Cold War, every single system we built, real big system that had to operate on the battlefield had to be EMP hardened, electromagnet pulse, because we assumed that the

threat of tactical nuclear weapons would fry your electronics so you had to have EMP hardened. And it was just built into everything. I was just a cost that we accepted.

Well, now everything has to be cyber and electronic warfare hardened. And all of the equipment that we have right now was built in an era where you really didn't have all these cyber threats, the internet of things, The DOD internet of things.

Rather than building up, the first thing I would do is let's get out there and fix all of our stuff in cyber, and I'm just using that as an example. There is a lot of different capabilities that I believe that we really have to get right, and then debate what is our theory of how we will operate in the world. What is the Trump administration on the theory of, you know, right now we have a wind hold forestructure, one big kind of military operation and a smaller one.

Well, for 20 years we had a two-war construct. So the incoming Trump administration will make those decisions, and only after that happens would I start saying let's build up the force because I can't tell you whether to build up the force until I know exactly what your theory of the world, you know, what is the U.S. role in the world. What is the foresizing construct that you want.

So I'd really focus right now on getting that right, and getting the capabilities, you know, throwing in some of the capability gaps that we have right now, buying more munitions, you know, paying a little bit more money on readiness and things, and then debate our role in the world, and then start the build up.

So my only recommendation is, look, a larger force, who's going to argue against a larger force? It gives you more buffer, a lot more stuff, but, you know, make sure you understand what you want that force to do before you just start building. That's, I think, the way I would approach the problem.

MR. O'HANLON: Excellent. Go over here, please. Sidney.

MR. FREEDBERG: Thank you. Sidney Freedberg from Breaking Defense. Hi. One of the things you've touched on is these are not Terminators. These are not Skynet. These are, the machines are always going to be in the life or death situations presenting information to the humans to help them decide.

And I think about people following their GPS into lakes, and even if the computer isn't maligned, if it's systematically wrong, and you go to trust it, you can go very wrong. And, of course, the (inaudible) scenario you may not notice you have a singularity on your hands until you've built your own cage, locked yourself in it and realized, oh, I just trusted the computer to talk me into that.

So how do you build decision aids that actually don't just embody either the biases of the programmers, or the emergent defects of the software.

SECRETARY WORK: So that's a great question, and one we're debating all the time. When DSBA, DSB, the Defense Science Board, when they came to us and said this is the competition you have to really pay attention to. You've got to go after it. So we've really worked on that and gone that way. Now, we've asked the DSB, okay, we want you to do a summer study on counter-autonomy and counter-AI.

On learning machines, for example, you can get into a learning machine, and you can dicker with it, and it will learn things that you don't want it learn, or it will do things that are incorrect.

So the next big step is let's make sure that counter- AI and counter-autonomy we understand what we're doing so we don't go down these pathways.

Another thing I always ask the chiefs is, look, you're going to have to select commanders for these new battle networks, these human machine collaborative

battle networks that are different than commanders who used to employ mechanized brigades on the battlefield.

And you've got to ask yourself, do you want a commander that just does what the machine tells them, or do you want a commander that listens to the machine, which gives options to you and says these are things you should consider, and the uses their experience to make the decision?

Now, for me it's not even a question. You're going to pick the second one all the time because if you're just going to have commanders who listen to a machine then go automatic. Right?

I mean, we believe we have an advantage in our people. We think that men and women who grow up in the I world, in a democracy, have an inherent advantage over men and women who grow up in the I world in an authoritarian regime because they are viewed as potential sand in the gears, and we view them as potential sparks of tactical and operational innovation.

So the questions that you ask, Sidney, are very important, and what you've got to do, like how do you do operational testing evaluation? How much of your operational testing evaluation do you have to do before you trust the computer?

Now, we don't, we don't really have that questions. But I'll give you a perfect example. I'm reading this, Horn Fisher, the guy who writes about the U.S. Navy in World War II. What a terrific historian. And he's reading the Fleet that fled Time. It's talking about the latter part of the Pacific War.

And they're attacking Saipan, and the air group commander of the Lexington says, okay, guys, we're going to go out and we're going to find the Japanese Fleet. If you see a carrier, you're going to attack the carrier. I don't care anything else

you see, you will attack the carrier. If you can't find carrier, the next thing you're going to attack is a battleship. If you can't find a battleship, the next thing you're going to do is attack a heavy cruiser. And if you can't find heavy cruiser, you're going to go after a destroyer, and if you can't find a destroyer, you're going to go after auxiliaries.

That's exactly what we'll tell autonomous machines, and they could do that darn good. It's not like the autonomous machine that says, okay, today I'm going to decide to go after an airplane. No. The autonomous machine will say you have these seven choices in this priority. I know there's bad guys out there. Go out and hit one of them.

A human is in control. The human designates the targets. The human sets the priorities. And you trust the machine, the autonomous weapon system, to do it.

We do that today, and no one should have any fear of that. The machines are not going to decide I don't like what my human told me today so I'm going to go attack this.

So your questions are very important, and a lot of debate, political, moral, legal. We will have many more strictures than our potential authoritarian competitors will have, and it's something that we have to watch.

MR. O'HANLON: Excellent. We'll go here, and then we got two more at least subsequently, and then we'll have to start to wrap up.

MS. CARTIER: Vernonia Cartier. I'm an individual researcher. I would like to discuss about is there any attention by DOD looking into Chinese maritime expansion to Asian countries, especially in Indonesia?

Recently, China investment of about $31 billion, and I believe it's aiming control for Strait of Malaca, and Strait of Lombok, which is provide access to Indian Ocean and Pacific Ocean.

In January, 2014, Chinese PLA Navy is upgrading it's destroyers and frigates to range further, and have been seen in the area the longest on previous Chinese landing ships along with destroyers in Strait of Lombok.

Would you please verify that, sir?

SECRETARY WORK: Well, let me break this into two parts, Veronica. The first part of your question really has to do with managing the strategic competition. So President Obama and his team, our team, has really been focused on that for a long time. We say that the Asia Pacific Theater is the most consequential region in the 21st Century, and it's how do you manage the strategic competition with China.

Now, let me just say for liberal democracies, we seem to think that competition is an inherently negative word. For both the Chinese and the Russians I believe competition is the natural state of international affairs.

So managing the strategic competition has to do with, hey, how will we approach the way the Chinese operating in the East China Sea or the South China Sea, et cetera. And because we're really focused on the third offset, I'd rather kind of stay away from that for right now.

It is true that the Chinese navy is growing by leaps and bounds, and they are pursuing many third offset type things. Lots of guided munitions, lots of battle networking. So we're really focused on that. We're saying as they develop capabilities, let's make sure that our capabilities are at least at parity, and preferably better to make sure that a collision is least likely.

MR. O'HANLON: Peter.

MR. CHUTLEY: Thank you very much for coming here. My name is Pete Chutley. I'm retired from Brookings. One of the big success stories of U.S. national security policy after World War II was to establish nuclear deterrence that worked.

Now, I think we have failed to establish cyber deterrence. The Russians clearly were not afraid to interfere in our election in this last year. What needs to be done to establish a system of deterrence in the cyber realm so things like that don't happen again?

SECRETARY WORK: Well, let me put it this way. And again, I'm going to go back to the framework of strategic deterrence, conventional deterrence, and managing the strategic competition.

And whenever you're trying to establish a stable, I mean, whenever you're going after comprehensive strategic stability, you have to know what the other competitor is thinking. So we right now, I will say, cyber is like the Wild West. Jim Clapper, the Director of National Intelligence, calls it the Wild West. There really aren't any international norms. It's kind of, you know, whoever makes the rules makes the rules. They do all sorts of different things.

But here's the difference. Strategic cyber is cyber that I would define as cyber that's going after the critical infrastructure of a competitor. Something really to damage their economy or their national infrastructure.

And operational and tactical cyber is really going after radars, and ships, and missiles and things like that.

Well, I believe what, to go back to your question, Pete, is that we believe, we think of operational tactical cyber like a tactical nuke. Our tactical nukes are in strategic deterrence.

The Russians conceive of tactical nukes escalation control. They think of them differently than we do. And so that's an asymmetry that we have to really understand, and the more you talk with your competitor and say, look, here's how we're looking at this, how are you looking at this, that's how you really kind of achieve comprehensive strategic stability.

I do not believe the Chinese and the Russians believe that tactical and operational cyber are the same as strategic cyber. We say, gosh, if you go, it's like dropping a tact nuke, and you risk escalating to strategic cyber, we're having a lot of tact (phonetic 1u:44:28) surfaces, we're an open country, it's a vulnerability. You've got to watch out.

Whereas, I believe both Russia and China see a distinction, and that they are more than willing to use cyber in managing the strategic competition for signaling, things like that. And I think what we have to do is just keep thinking this through.

To get to deterrence, we have to understand the way our competitors look at it. We have to talk, establish norms, and that's the way you will get to this.

So I think we have a way to go. I think the Obama administration has been working hard on that. I believe after, for example, when we indicted the Chinese cyber actors, it really had a change, you know, it had a change in what the Chinese were doing.

So we just have to continue to work this out. I agree with you that we have a ways to go.

MR. O'HANLON: So we've got two last hands up, and I'm going to have to take and end it there. So here in the third row, and then maybe the gentleman there in the sixth row. If you want, you can take them together, and then have one grand finale.

VOICE: Hi. (inaudible) with Aviation Week. Last week we saw congress with a defense policy they'll split Frank Kindel's position into a chief acquisitions officer, and a chief technology officer. So how do you think that having this new position of chief technology officer to do innovation and outreach for Silicon Valley, how do you think that will impact third offset, and you think this is a good thing for the DOD? I mean, how do you think this is going to play out?

MR. O'HANLON: Great. And then together with this gentleman's question back here.

MR. BATES: Zack Bates with Jane's. I wanted to ask you, you just described the separation of operational and tactical cyber from strategic cyber.

You also mentioned earlier about concern that adversaries might get into AI systems, or in some way manipulate them to harm our capabilities, U.S. capabilities.

Do you currently think that the operational and tactical networks that the U.S. is using are trustworthy? Do you trust them fully, or do you think that the capabilities you described with Russia and China having grown considerably have made them untrustworthy? And if you don't have full faith in them, how do you manage that lack of trust?

SECRETARY WORK: Well, let me take the second one first because the first question really is about organization and stuff.

Do I trust our networks? Yes. But do I think they're going to be under attack if we ever do get into a situation like this? Absolutely. And I worry about the DOD internet of thing because with all of the things that we have today, we're really not designed to withstand these type of attacks.

Now, before I became the undersecretary of the Navy, I was at CSBA, as Michael said, and for about a decade, I was heavily into war games. And in every war game, the red would always attack our battle networks.

There were two schools of thought. One school of thought said, hey, you want to spend a lot of effort trying to maintain the network at full operational capacity.

A second school of thought said it's a fool's game. Assume that your networks will devolve into smaller tactical battle networks, and work for thin line communications between them so that you can have a coherent campaign (inaudible 17:47:52.

In my view, the second school of thought always won. When you are focused on the network, you're focused inward. You're not focused on your adversary. And that's a bad place to be whenever you're in a tactical fight.

So do I trust the networks as they exit now? Without question. Do I trust that I'll have my full network in the first hour after a conflict? No. Do I trust that our forces are trained for that very output, outcome? Yes.

So I think I'm okay. I think I worry about it, but do I trust them? Absolutely.

Now in AT&L, the NDAA was signed last I think Wednesday night, and I went to the Regan Defense Forum, and so I worked all through the weekend, and I still haven't gotten a full readout. This is going to sound like a dodge, and it is.

I just haven't had a full readout so I don't understand exactly what congress has said. I have heard two different things. That we have to establish it right away. And then I've heard another one saying, no, it's really not like that. Congress is saying you have about a year to think about this.

So what I'd say is I need to really look at this first. At first blush, I do not think a separation is the way I would recommend, but it might be okay once I see what's in the bill itself.

We're debating that right now inside the Department. You know, is this something that we should say, hey, this is a good thing, or is this a bad thing. We're debating it. So I can't give you a perfect answer right now.

MR. O'HANLON: So in just a moment, we're going to shift to our second panel, but before we do, please join me in thanking Secretary Robert Work.

SECRETARY WORK: And, Michael, thank you again for doing this. I had a great time. And thank you all for thinking about this.

You know, these are big issues (blank tape 17:50:03).

MR. O'HANLON: Thank you, sir. (Applause).

And as Kelly and Alan get mic'd up, I'll thank all of your, those of you who are able to stay. We've got another hour on this topic, and we're looking forward to a discussion with you.

We'll have a very similar kind of framework where I ask a couple of opening questions, and then we go to your thoughts and questions and comments as well.

And so let me now, please, introduce Alan Easterling and Kelly Marchese. Kelly is with DeLoitte. She is an expert in efficiency in organization and in

manufacturing. She is a graduate with an MBA from Duke University in these kinds of issues. She is a black belt in Six Sigma efficiency. In other words, trying to make corporations lean, trying to make DOD innovative and effective across it's bureaucratic but also its manufacturing sectors. And obviously, therefore, issues of innovation both at the organizational level and the technological level are crucially important to what she thinks about, and all of these have been teed up nicely by the Secretary.

Alan Easterling is with Northrop Grumman, although for the first part of his career, he was in the U.S. Navy as a Captain, and wound up with some stints in Applied Physics Lab and also other place where he thought about undersea robotics, as well as many other areas of technology. So he also has a technical background, in his case more in the hard sciences and engineering. Naval Academy graduate before that.

And so we're delighted to have them today, so thank you Kelly and Alan, and we'll launch right in. I think the best way to begin is just by asking you to reflect on what you just heard from Secretary Work.

So maybe, Kelly, over to you with just some broad impressions, and, you know, if you need a more specific one which I doubt you do, but I'd just like your broad impressions, but I'm particularly interested in how we should think about the Secretary's definition of technical innovation with this concept called the third offset, whether it sets up correctly as we're at this transition point going into the Trump administration.

MS. MARCHESE: Michael, I've been looking forward to this. I really enjoyed Secretary Work's comments, and when I think about the third offset, or, really, the future of anything, you know, we often default to talking about the technology because that's the sexy side, right? You know, the shiny new objects.

But if the goal of the third offset is to create an enduring strategic advantage, it can't just be about the technology because that can be replicated, copied, or mitigated by adversaries. We really believe it's all about the architecture, and how those different technologies are integrated, and so I really like what he had to say around the importance of the, he called it operational and organizational constructs.

I think that's critical. We spend a lot of time focused on our R&D budgets on the technologies and less so on architectures, and those architectures are how we structure those technologies, and how they communicate and connect with one another.

MR. O'HANLON: I've got a follow up. I should have said, by way of introduction both Deloitte and Northrop Grumman are important members of our ongoing industrial based working group we have here at Brookings. We're grateful for their intellectual and financial and every other kind of contribution. As you can see, we have a lot of expertise reflected in who's here today.

What I wanted to ask was how would you evaluate where we are in trying to make the Department of Defense more efficient and effective organizationally because as you say, it's always easier to talk about the technologies, and we can certainly think back over a half century to the invention of nuclear weapons, and satellites, and stealth, and precision strike, and cyber capabilities, and all the things that the Secretary was talking about, and most of us do form an image of each decade, at least I do, based on which technologies came into being then.

The Secretary did mention, or alluded to jointness, and, of course, Goldwater Nichols, which is seen as a big breakthrough. But beyond that, how much progress have we made? Is this organization still this behemoth that's unmanageable and unauditable and we get lucky when anything actually does work organizationally, or

do you detect a real progress that even though there's still a long ways to go, you know, you can say that DOD operates better as an organization or as a system of organizations than it might have 20 or 40, or 60 years ago?

MS. MARCHESE: So I should mention, I've spent most of career working on the commercial side, so only recently on the federal side working within the DOD space.

And so by comparison, the federal government is much larger, and so it is a little slower in the way that it can connect. And I think that's been okay in the past because of the size and the scale and the investment in technologies.

But if you look at the speed at which things are changing, agility becomes that much more important. And so on the commercial side there's a lot of drive of those technologies, yeah, it feels like the focus in order to enable those technologies has got to be about the connections of those technologies. And the federal space has a unique position where standards haven't necessarily been set. They can help set those standards. They can be on all sides of the avenue.

Jointness is a great term, but it's probably not going far enough in order to keep up with the pace that needs to happen.

The other thing that I thought was really interesting is the focus of the third offset is around the conventional deterrent, so it's about the large state actors. But those aren't our only threats, and our only adversaries. And so agility becomes even more important with those other adversaries.

MR. O'HANLON: One last question before I got to Alan.

So are there examples within DOD of places that get it more right than others, and, if so, is it just because the, you know, smallish, you know, Joint Special

Operations Command, or, you know, whatever your favorite may be, or is it because of specific lessons they understood or the key leaders were able to implement, whereas the rest of the organization in the Department of Defense universe hasn't yet had those breakthroughs, hasn't yet had those key leaders, or is this so big that inevitably it's going to take longer?

MS. MARCHESE: So one of the places I have seen great progress is in some of the innovation institutes that have been created under, it's public private partnerships. So it is where public and private organizations are working together. So Manufacturing, it's called Manufacturing USA, so there's a number of different innovation institutes that are focused on different technologies, and so it is pulling together academia, federal agencies, as well as industrial members, and that is jump-starting a lot of the learning and driving the technology and the coordination across industry a lot more quickly.

It's forcing them together to do projects instead of each operating in individual silos and solving the same problem in parallel.

MR. O'HANLON: And you can identify certain areas of the country whether it's Silicon Valley, or Albuquerque, or North Carolina, what have you, where some of these innovation clusters are in existence?

MS. MARCHESE: Absolutely. Absolutely.

MR. O'HANLON: So Alan, thank you for being here as well, and may just like your broad reactions to where you think the third offset is right now, and just any other reflections after hearing Secretary Work.

MR. EASTERLING: Let me dismiss with the cultural and the organizational first, and then I am going to come to technology.

You know, as an old Navy hand, I enjoyed some of Deputy-Secretary Work's observations about the Navy. Particularly from a societal standpoint, I'm a cold war product, and we became quite interested when the Soviets began advancing their capabilities in naval aviation, and we watched ships like Admiral Kuznetsnov get underway and demonstrate some capability.

Now, we weren't terribly worried. I mean, what we were waiting for was for the Soviet navy to invent the chief petty officer. When they invented the chief petty officer, you have reason for concern.

From a cultural standpoint, the Soviet Navy also was proud of saying that they had a copy of our battle plan for war at sea, but they tendered the xerox somewhat ruefully because they were aware that the U.S. Navy had never read it.

And the companion piece to that is war at sea is chaos, and the American Navy practiced chaos at sea everyday,

so that these cultural elements that tend to segregate us from our adversaries.

But here's the important piece I think about what I heard. And the subtext of this conversation is what next for the third offset.

I don't think we have a choice, right, because what I enjoy about the third offset terminology, and, Michael, I very much share your historical perspectives on this as well, the first offset, the second offset, the third offset is that each reflected sort of a conjunction of historical and technological inflection points, and I think I heard one of those inflection points today.

But I think the critical difference is if there's technology inflection points in the first offset, and then the second offset were driven largely by domestic defense spending and investment.

That's not what's happening now. If you look at that laundry list of technologies, synthetic biology aside, right, and perhaps some words on that later, but if you set biology aside, and if perhaps we set aside autonomous weapons, the leaders in the development of those technologies by and large are in the global technosphere, something that didn't exit at the time of the first offset, or the second offset.

I made comment at the high tech caucuses, and a conversation I had with Vint Cerf at Google. And Vint made the observation that at Google they had the pedal for the medal on artificial intelligence. They had 1,200 researchers, that number could have doubled by now, who knows?

At Northrop Grumman, we're terribly interested in artificial intelligence, and we have researchers, but we can't put 1,200 people onto the job. That's a global interest, and so the Secretary is quite right as is the Defense Science Board quite right to focus upon that aspect of technology because it's being driven globally.

So you don't really have a choice. You can't pretend like it's not happening. And all of the subsets of artificial intelligence, right, the cognitive process, the machine running, however you want to cut it up.

That train has left the station. And to emphasize too, this time it's global. The previous word, "domestic." And global service is all comers.

So it's almost as if the offsets that we were developing were nullified by the ubiquity as they were being developed. That's the situation that we're in right now.

MR. O'HANLON: Interesting. Where do you see the greatest promise right now in terms of being able to deal with both vulnerabilities and opportunities? So you have a background and ongoing interest in undersea robotics, for example.

MR. EASTERLING: Uh-huh.

MR. O'HANLON: And to me this looks like a fascinating domain of future warfare because one thing we know about the oceans, people talk in sort of simplistic, casual ways about how we're going to make them transparent, I don't think we're going to make them transparent.

But we can populate sensors much more widely, and even that is going in a sense back to the future because we did this with Sosis already during the cold war. Put a lot of effort into it, had a lot of listening devices, all over key parts of the world.

Now, we're thinking of being able to do some of this with mobile, robotic platforms that maybe come back to a mother ship or what have you.

Is this one of the areas of greatest promise, one of the areas where we have to, you know, expand our thinking and really devote a lot more resources just to take one example.

MR. EASTERLING: Without question. And it's a priority within Northrop Grumman. Somewhat surprisingly given that we had a submarine business and spun it off as part of (inaudible).

So we're thinking about the problem absent the submarines, which is actually a very hopeful way to approach it. I mean, what build rate, one-and-a-half ships a year? And that's at a replacement rate, I think. It would be very difficult to build at a cold war pace. To have the number of holds in the water that we need to confront this problem. But there's another dimension to this, and either surface ships in my view are becoming increasingly vulnerable. And my touchstone for this is the Falkland's War of 1981-1982 time frame, right?

And granted we were in a different world, a different type of technology, but I still think there are many wonderful lessons to be extracted from that war.

And my most simple lesson from that war is the missile (inaudible). The interesting thing about the missile is it's not human constrained, you know, to the very good discussion about the defensive posture for automated systems.

Now, we're a long way from the (inaudible) of 1981 although it's still a quite capable weapon. We're now (inaudible) BF-21s. And so hypothetically, any surface vessel that comes within 1,200 nautical miles of a determined opponent in the future is at risk.

That would tend to push us underwater. It almost becomes the last bastion of stealth. But it's a tremendously expensive place to operate, and it has two significant technical hurdles left to be overcome: energy density, nuclear power plants aside; and communications.

We haven't cracked underwater communications. Extremely low frequency isn't going to do it for the battle networks that we need. So significant resources are and should continue to be expended.

Now, how can you work around that? Well, your surface operations, for example. Take advantage of overhead. Take advantage of air breathing assets. Take a combined approach to this so you're not just focusing exclusively upon those things that are wet and underwater, but that those things that are in the air above it that enable what's underwater, and the (inaudible) distributive approach.

This too gets us a little bit away from technology back to some of the observations Secretary Work is making, and that we need to take advantage of these systems to deceive, because one of the most frightening things about undersea warfare is not knowing where the submarine is.

And it's astonishing to see how people would behave if they even suspect that there's a submarine in the water. Most of my background is in antisubmarine warfare.

And the Falkland's War is a wonderful example where the Royal Navy as I recall expended nearly all of the submarine counter measures within the first week or two of the conflict because every time they heard something in the water, they thought it was a submarine.

That's the sort of uncertainty you want to bring to the battle space. That's the sort of uncertainty that you can take advantage of within the secrecy of underwater stealth.

But cracking those two problems, the communications and energy density, is at the top of the list.

To that end, DARPA has a program underway at the moment called (inaudible) in which they're looking at how we network these assets in just the way that we described.

MR. O'HANLON: I want to ask about two more vulnerabilities. One is going to be land bases, especially in forward theaters, and the second is going to be about cyber.

So I'm going to begin with the land bases, and then I'll pose the cyber question to both of you.

Before I do, I realize I was negligent in one other way. I needed to convey the apologies of Secretary Bill Lynn, who as you may have noticed was supposed to be on this panel, but he works with a company with a home in Italy, and you may have

noticed some things happened there in the last 24 hours for which Bill has to speak with his colleagues back home in Rome, and so he sends his apologies.

But anyway, I will continue to have fun up here. I think we have plenty of brainpower, and with all of you, we'll have some great additional questions as well.

So let me just finish up my part with the questions about vulnerability of forward land bases, and missile defense, specifically, because, Alan, you just mentioned that the ship is becoming apparently more vulnerable in the missile age, which I tend to agree with, but also this now raises the concern that land bases are becoming much more vulnerable everywhere from Taiwan to Okinawa, even the Persian Gulf with Iran's capabilities even if they're in an order of magnitude less than of China's, and certainly the Baltic Sea if we think about Russia's scenarios, and so my question would be, you know, are land bases inherently vulnerable, or if we do enough cleaver things with hardening, dispersal, short-take-off aircraft, you know, combined with waiting for that day over the rainbow when directed energy missile defense finally becomes available as people have been promising for a long time that maybe we can still stay forward, or are these forward bases really just in a sense, making sure you've got a trip wire, and if you ever get to real hardcore hegemonic war fighting it's going to have to be from bases that are further back. Do you mind taking that?

MR. EASTERLY: Well, I think -- so I'd offer the Philippines in 19141 as a case in point. It turned out to be a bit of a trip wire, right? It was intended to be a forward based, but it was quickly overwhelmed. Granted, advantage of surprise, it surprised to a (inaudible) warfare I believe absolutely it is.

I do think that the (inaudible) Mountain, and the deliberate two to three-month buildup without opposition is anomalous. I think that the most coherent tragedy

I've heard for dealing with this problem is distribution. But if you're looking at a place like the Pacific, distribution where?

The age of the medium range ballistic missile with conventional warheads changes everything in this regard, I think.

We haven't faced an opponent who built their defenses around those capabilities with every intention of using them. So we've had this luxury of time, and we've had this luxury of logistical mountains. And I think that just plays very heavily in Ward C, right, because naval ships are still dependent upon resupply and refitting ashore. (inaudible) combat ship. In order to change a module, it has to go into port. That doesn't happen at sea. Even (inaudible) ship after the 120 silos are expended, it can't reload at sea. It goes back to port to reload. And given the nature of the combat that we expect in that part of the world, they will have to reload. And they do expend those silos very quickly.

So one thing that we have to contend with, it's an excellent question, is the matter of logistics and resupply at distance in a theater that is all about distance to begin with where you're being held at risk before you can even employ your own weapons.

MR. O'HANLON: Let me now turn to cyber and ask Kelly and Alan both about this. And I see my good friend, Brendan Orino (phonetic 18/09/14). Brendon was the research assistant to our former colleague, Peter Singer, who wrote a book called, "Ghost Week," that a lot of you, I know, have read in which he basically made the argument that the entire cyber infrastructure of the U.S. military is far less dependable as Secretary Work just asserted.

By the way, if you were deputy-secretary, you might feel like you needed to say that whether you fully believed it or not, and I'm not in any way suggesting that he doesn't believe it, but it's a fair question for all of us to worry about. To what extent have we built up a cyber infrastructure in the U.S. military that in crucial ways is going to fail.

And, again, Secretary Work actually did give a lot of nuance to his answer when that subject was raised because he acknowledged that a lot of your networks are not going to succeed, not going to survive, and what you have to be able to do is fall back into a more modest capability where localized or tactical networks, perhaps, survive and can talk to each other to some limited degree as is necessary. Maybe that's the best we can hope for.

But whether it's at an organizational level, or a technical level, or both, I would just love your thoughts, you know, and to put in a fun way as Peter Singer right, that we're in a world today where we actually could see, you know, most of our cyber infrastructure basically taken down and rendered not only temporarily disruptive, but almost useless for a major conflict, you know, and if so, is there anything we can do about it?

MR. MARCHESE: So I'm going to talk about the cyber implications on logistics and maintenance, right, so there are cyber implications on defense systems and military systems, but if you think about one of the things that's really important as sustainment, and maintenance and logistics. And so cyber implications on that part of our operational organization.

And I guess there's a good news, bad news story. The good news is because so much of that is not connected right now, it would be really hard to have a broad-based impact on that.

The bad news is, it's not really connected and it needs to be in order to operate as effectively as the direction of all the internet of things is leading us in that direction, and giving us the capability for it. But we don't have that connectedness yet.

Once a holistic strategy is put together around what that architecture should be, it can be around any kind of defense network, but if you think about maintenance and logistics, the cyber side needs to be covered as well because that digital supply network will have sensors that are always on, you know, they're constantly transmitting data and information. There'll be communities. They're sharing all of that information. There will be machine insights and human insights, all those things that Secretary Work talked about, you could work against it. Those things could work against you if they are not protected by cyber. But first you have to connect them in order to protect them.

MR. O'HANLON: Let me just tease this out a little further because, and you're a great person to ask because it's sort of where Six Sigma collides with vulnerability, and the Six Sigma in you wants to see everything be optimized and efficient, right?

But I've heard people say one of the things they like about the old ICBM is they're not efficient, they're not, the cyber isn't that modern. Thank God. Because if you wanted to attack them cyber, you probably can't even get into that old IMB mainframe or what have you.

So are we really well advised to try to tie everything together and hope that somehow our software, or whatever else we do by way of defenses is good enough to protect us, or are we better off staying a little bit unconnected and inefficient, but at least we can't be vulnerable to that one sort of brilliant strike.

MS. MARCHESE: Yeah. I'd be fine with that if it was by design, not connected by design, right, as opposed to by accident, or because we haven't taken the time in order to do that.

We've got, I mean, it's not about just the technologies. We've got the -- to Secretary Work's point, we've got the cleaver people out there that will help us think through those areas where we, where do we need to be connected,
how can we best network, and how do we leverage insights and make the right decisions if that's an area of focus.

So, again, I go back to the architecture piece, that holistic architecture is where there hasn't been as much focus as each of the individual silo technologies.

MR. O'HANLON: Great. Alan, any comments on the board issue of cyber vulnerability?

MR. EASTERLING: Yeah. To me it looks like another variant of the electronic warfare conundrum where you have electronic measures, and you have electronic counter measures, and you have electronic counter counter-measures, and so on. That's never going away.

And cyber looks the same to me. It is built into the system for better or worse. And I see it only becoming increasingly problematic, as it becomes increasingly dependent upon the very real advantages that these systems bring us, and as cyber itself matures as another domain of war.

You know, the Secretary was also, I think, carefully navigating the implications of cyber war. I mentioned Insurf, who also cautions against using the term, "war," with cyber. It tends to pervert the thinking. It's not war. You need to come with a whole new language to describe what's happening there.

At every given instant in time, there are millions of machines all over the world who are interacting with one other, who never knew the other machine existed, and perhaps only did for those few seconds of exchange it will never connect again.

There's this extraordinary neural layer to the world, right, (inaudible) to call it the neural layer of the global economy, right, is running behind the scenes to which we're largely oblivious, but we've created it.

You think about the fact that 90 percent of transactions on the street, that's a rough figure, right, are machine-to-machine flash trading. We've already let this out.

And the system will inevitably have vulnerabilities, the system will inevitably have exploits, and we simply need to factor that into our planning so that we are able to contend with graceful degradation, if there's such a thing. It's a hopeful word. And alternatives when they begin to lose access to these systems. But the systems in general convey speed, and they convey knowledge without which we can't fight.

I thought Sidney Freedburg's question was wonderful because behaviorally what he was suggesting is exactly what people do.

I was on a panel the other week with (inaudible) systems. And we were talking beforehand about the work IBM is doing at Watson. And Watson, you're familiar with the (inaudible) has gone to med school and is practicing oncology. What Watson is able to do is keep up with all of the literature that the harried and very busy surgeon can't keep up with, and has access to all of the visual case histories on the planet, which the surgeon couldn't read if he wanted to spend a lifetime.

And Watson find pattern that the surgeon would not otherwise find. And Watson has become extraordinary at delivering accurate diagnoses and therapies that would never occur to the surgeon in many cases.

The same technology is being used for nurses for rather routine monitoring the patients in intensive care wards. Here's the thing. In the early experiments, it doesn't take long for the nurses to become entirely dependent upon the AI and simply, well, it's always right. So whatever it said. And they're less inclined, especially with fatigue. Now, let's think about the battle space when they're under pressure. Again, just think about the battle space to question what the machine is telling.

Now, it has already been such with machines, I think. Until you get to a point of absurdity where you say that can't possibly be (inaudible). Don't drive into the ocean, but some people do.

But the thing about Watson is it's a network device. Everyone doesn't get a Watson. And I see a future in which the Defense Department increasingly goes down this type of model. In fact, I've heard Secretary Work talk about doing just that, where you're drawing your AI from a network which itself is subject to exploitation.

But the sheer power of that AI is going to force (inaudible) use that network. You just have to come up with the necessary countermeasures, counter counter-measures, and so on. That will be part of future war.

MR. O'HANLON: Thank you. I'm about to ask you for your thoughts and questions, but I've got one more big picture for the panel, which is, okay, we are at this milestone in American defense policy under the Obama administration, and presumably the end of the Ash Carter tenure at Psych Def (phonetics). We'll see about Deputy-

Secretary Work. But this raises the question of how do we take stock of the third offset. And what has it meant? This is not to be disparaging in any way, but every administration needs its own bumper sticker, and is it essentially just the Obama administration's or Deputy Secretary Work's, along with his bosses and colleagues, or is there something to you that's distinctive about it. He emphasized artificial intelligence and organizational change, and sort of a grassroots approach to innovation more than anything more specific or technological.

But is there anything about the third offset that for you is the most memorable, the most important, the most distinctive, and, therefore, he most crucial to build upon going forward?

And if you want sort of a wrap-up question, is it going to survive? Is this a term that is actually, has any chance of being used by the Trump administration?

So Kelly, within those broad questions, how successful has it been? What are its chief attributes? What does it really mean to you? What are its prospects?

MR. MARCHESE: I do think it has been, it's raised a question that needed to be discussed, and I do think it's made definite progress. In terms of the Obama administration, there has been a recognition that in order to stay ahead of our adversaries, we have to operate differently. Not just be technologically advanced, but how we develop those technologies, how we work together across federal and commercial, we need to operate differently.

You hear the term, “ecosystems," all the time, public and private organizations working together, and that will help us because the third offset is about an advantage for the United States, there's a lot of commercial organizations that want to maintain that advantage as well.

And I wouldn't be surprised if it didn't continue into the Trump administration. It seems to be aligned in terms of making sure that there's kind of strong positioning against our adversaries, so I'd be surprised if it doesn't survive.

MR. O'HANLON: Alan.

MR. O'HANLON: I think the word we're looking for is what makes it enduring, and I alluded to this in earlier remarks. I think one thing that makes this enduring is the nature of a dual inflection point, and the acknowledgment of our own vulnerabilities. Having acknowledged our vulnerabilities, we can't very well just throw our hands up in the air and say, well, we'll live with it.

Land forces. We talk about land bases. I mean, our armored forces are not geared towards operating in an environment where the opponent has the same sorts of precision weapons that we enjoy. It does not.

Would we put them at risk in that environment? Would you put the amphibious navy at risk in (inaudible) landing today given the sorts of precision guided weapons (inaudible) in the world today? I rather doubt it.

So you wind up with huge generalizations here, which I apologize, whole segments of the armed forces that unless you're willing to accept risk which historically we've been reluctant to undertake which are unemployable in the world that we're forecasting.

And then you have rebels in Yemen who are actually employing guided missiles off of their coast right now. You don't need to be a nation state to gain access to (inaudible). Perhaps it helps you to be a little more effective, but you don't need access, a nation state to have access.

But the other piece of this is the rise of the global technosphere, which I'm to revisit. That's technology for everyone. And those who are unburdened by existing defense establishments, and have the opportunity to observe how we have fought for decades, what our vulnerability are, are the ones that should give rise to most concern, and they can do it on the cheap, if you will.

They don't need a massive R&D establishment such as ours. It's available globally to them. That doesn't care what administration is in power, and it's just as real, and it contributes to the vulnerabilities that I mentioned earlier, those who've observed how we fight.

And finally, many of the types of warfare that we're talking about tend to be an outcome of America trying to project power into very well-defended enclaves where we have not only the tyranny of distance, but they had disadvantage of being the attacker, which also puts us at a significant disadvantage.

These questions don't go away. And I think the shape of the answers are persistent. They're enduring as well, and they draw from this global technosphere.

MR. O'HANLON: Thank you. Well, let's go to you. Any question under the sun that relates to innovation is fair game. And you can pose to anyone of the three of us as you wish, but more than one may respond depending. And maybe we'll take two at a time. See how we do that way. So we'll start here in the third row, and please identify yourself first.

MS. FRIDAY: Hi. My name's Joanne Friday (phonetic 1823:09. I'm retired from a career on active duty in the Air Force. That's basically the stance I'm coming from.

I just wanted to point out when you were talking about do we, should we be interconnected, should we be networked, is it safe?

We launched jets and sailed ship for many years without being networked. We didn't know what a network was. We used to exercise all the time. If the network went down, how are we going to launch the jets?

So, yeah, we had to do that regularly. I think still in the year 2016, one of the reasons why we still don't have a lot of interoperability is because when computers first came into the service, the DOD, all these contractors came to our commands and said, hey, we got a solution for you. Here. Use my system. So all these systems came everywhere and still nothing talks to the other system.

So we're still dealing with that, aren't we? And there's a lot of fallout, and it still causes problems for people in uniform. So I just want to make that observation.

MR. O'HANLON: Thank you. Take one more and then we'll have responses.

VOICE: Hi. Nicholas (inaudible). I'm an independent contractor for the satellite industry, and I wanted you to expand a little bit upon the proliferation of broadband as we're seeing come on line, as well as the use of broadband in emerging economies.

MR. O'HANLON: Kelly, you want to start with either of those or both, and then we'll --

MS. MARCHESE: Sure. Well, I mentioned I think it was (inaudible) made the observation about systems that don't talk to each other. That is not unique to the DOD. So commercial organizations face that as well where they have had lots of different systems that have grown up, legacy systems grown up over time that don't

necessarily connect. Companies make different acquisitions, and they're all faced with the same problem, but they don't say that's a strategic advantage.

They absolutely recognize there is a huge advantage to being interconnected, and its part of their, the way they operate their business is finding the ways to drive that interconnectedness. You need to be able to have a fall-back plan for when things may go wrong and are not connected, but there's too many advantages. Again, going back to would you rather not be able to have information feeding back from your equipment about whether it's about to fail? Would you rather not know that, or would do you see an advantage to knowing that in advance?

MR. O'HANLON: Alan, care to comment?

MR. EASTERLING: Yes. I mean, obviously there was a time when we could operate without the networks that we enjoy today. I think that's about as relevant as to the days we operated before the telegraph. It's just a different world.

In the Navy, I'll offer the Navy as a case in point. We talk about launching aircraft without communication. Well, the Navy's response to the ability of the Soviets to collect overhead intelligence on RF transmissions was the MCON policy, emissions control policy. And so you would lock the ship down. The ship learned to fly aircraft, to launch and recover aircraft in the middle of the ocean thousands of miles from anywhere without reference to any radios. There were no emissions from the ship, no emissions from aircraft.

Ships sometime hard to find. I would challenge the Navy to lock a ship down today. Not they would typically want to. We have to, I think, appreciate the vulnerabilities that we have, and learn to work with them and around them.

It's much like the information layer, the neural layer of the economy that I mentioned before. This is the neural layer of the global economy. It is the neural layer of our war-fighting machine. And I don't see us going back in time.

(inaudible), as I suggested when you not have everything that you're accustomed to having, but the (inaudible) only, and I don't forecast the day when they operate at midnight, as we used to call it in MCON 4.

The question about -- I'd like to expand the broadband question actually to hit the satellite because we haven't talked about that very much. And we are as dependent upon overhead as we are on the networks that we're talking about (inaudible). They're connected to one another. That's the answer to broadband.

And what's really interesting about what's happening in space beyond our vulnerabilities as a space-dependent military is the extraordinary companies who are (inaudible) so many satellite models and planet wraps comes to mind. And not surprisingly many of these companies are coming out of the valley and it's not a cell phone-driven revolution. Many of the technologies that run your cell phone are now in orbit, in small sets, in nano sets, and you get private companies such as GOI, who are able to provide intel quality imagery not just to nation states for whom they will subscribe, but to individuals.

If George Clooney wants to raise interest in what's happening in (inaudible) pass over Sudan, he asks for a collection pass over Sudan, and he gets it. That's a kind of individual empowerment, it's happening, which is part of this inflection point, which is part of this global technosphere that I referred to. Satellites for everyone, if you will. And so broadband is just one piece of that.

MR. O'HANLON: Thank you. Another round. Anybody else? Harlan.

HARLAN: I'm Harlan. I'm going to ask you an impossible question so be prepared. I've asked this to any number of people, including Ash Carter and Bob Work, and they go purple.

At the Regan festivities this weekend, Joe Dunford, the Chairman, said that we are prepared to be able to defeat any one of the four following adversaries in war.

If you were advising the Pentagon today, how would you go about defeating Russia in a war in which nuke (blank tape 18:29:00 to)?

MR. EASTERLING: Yeah. I think, not to dodge the question, but it begins with what do you mean by defeat? I mean, we have this mentality that seems lost in 1945 where the way these things end is you take the opponent's capital, Berlin, Tokyo, and that, you raise your flag, and you look around, and you wait for your liberal western democracy to emerge, and then we're flabbergasted when it doesn't happen, because it happened in 1945 at least once.

I don't think we know -- and I would submit that that was an aberration from which we've drawn far too many lessons. And if you look at all of the intervening history, I'd look at every conflict to which we've been a party and ask what did it mean to defeat the opponent.

You know, if the question is rather what does it take to prevent the Soviet from employing -- listen to me. I'm a product of my past. I'm sorry. -- Russians from employing nuclear weapons, I mean, that's just, that's a different question. That's a matter of deterrence.

And two, what does their calculus say? What does it mean, what does victory mean to the Russian government? So then not to dodge the question really, but I think we have to ask ourselves how does this end.

VOICE: (Off mic.)

MR. EASTERLING: Yeah. Yeah, I think we find out --

VOICE: (Off mic.)

MR. EASTERLING: Yeah.

VOICE: (Off mic.)

MR. EASTERLING: Well, I'll give you one which actually comes from former Prime Minister (inaudible). He said the next target is Transnistria at which point most Americans look up from their breakfast and say, what? Transnistria? I don't think I care which is exactly why Transnistria is the next on the list. It's not the Baltics, per se.

That's a tough one. That's a very tough one. I'm not going to turn purple, but that's a tough one. How important is that? You're saying test of will in Syria which is arguably much more important than transnistria might be.

And I think that we're seeing a segue into a mode of thought in this country that says, you know, I used to be very interested in defining the world order as a matter of principal. I think I'm going to have a rethink.

MR. O'HANLON: Kelly, care to comment?

MS. MARCHESE: This is out of my area of expertise, and I'm thinking about all the shows that I watch about people infiltrating the organization, and I really hope there's somebody in there that will prevent that from happening.

MR. EASTERLING: If I could revisit, I'm sorry.

MR. O'HANLON: Yes.

MR. EASTERLING: The other thing that's quite interesting, you know, we talk a lot about future war. That's one of the things that we do at the company.

Sometimes you don't have to write a novel. Sometimes you just read the papers and watch it happen.

And whether we call it hybrid war, nonlinear war, I am absolutely fascinated at the evolution, by the evolution of ISIS and the operations that we've seen in Crimea and Ukraine.

And I suspect that the answer to the question lies more in how do you contend with that than it does in a more conventional question of how do we avoid escalation (inaudible) warfare.

MR. O'HANLON: I'm going to take a crack at this too, if you don't mind, Harlon, and I also invite you to comment yourself on your own question once we're done.

So I'm going to mention a couple of different countries and different scenarios. If hypothetically Russia moved in to take a sliver of eastern Latvia, let's say. Just a sliver. And the thinking might be are the Americans and the rest of NATO really going to bother to liberate that sliver when it's going to take them six months to prepare, and maybe can hit a few of their ships with conventional weapons as they're coming over.

And then they run the risk, and we'll bluster and threaten nuclear war the whole time, they run the risk of starting a process that could lead who knows where. And we all know from Thomas Schelling the threat that leaves something to chance, if the Russians present us with a fait accompli even though they started the war, we have to sort of think hard about whether to start the counter attack, or somehow live with this aggression, which is part of why I think it's actually a serious thing to worry about because Russia probably wonders if a lot of NATO countries would have the gumption to respond, and I'm not sure I would recommend it for us.

In that scenario I just mentioned, I think that perhaps putting a substantial forward defense in central Latvia, Lithuania, Estona, Poland, in other words, not liberating but accepting that initial Russian attack, but then gearing up for another cold war with a full range of economic sanctions and choosing not to retaliate militarily but to make our forward defense quite robust might be the smarter answer. And maybe we're on the way to doing that with the European reassurance Initiative where we're going to have people in place. It's going to be harder to attack the Baltics and, therefore, the transnistria scenario is more credible, as you were saying, Alan.

So that's how I would think about some of the scenarios. You could imagine others that are much more egregious where I think we would have to respond in a symmetrical military way in Europe.

But just two others very quickly. I like the third offset as I said earlier, but one thing that I do worry about is if we think we can preserve the level or restore the level of invulnerability that we had in the western Pacific in the years before China was a high technology military, I think we're deluding ourselves. There's just never going to be a return to that day.

And I hope the third offset doesn't make people think otherwise because some of the language that's employed to describe it is about preserving or restoring our conventional superiority.

I think it's going to, hopefully, be superior in some sense, but it's never going to go back to the point where the Pacific is an American lake, and you're essentially invulnerable to the Chinese when you're within visual sight of their homeland.

So that would just be to me an important premise to put on the table. And again, I'm going to give both of you guys a chance to respond here in a second.

And then my third scenario, the third country of concern along these lines is even the relatively underdeveloped country of North Korea because even though they don't have the ability to play in high tech sectors, they do now probably now have 15 or 20 nuclear weapons, which means that the possibility of assuming that any Korean war ultimately leads to the complete defeat of North Korean and the elimination of its government, and the reunification of the entire peninsula, this to my mind may no longer be realistic.

And there are a lot of scenarios we may have to actually live with a North Korean rump region at least, even after hostilities because risking ten nuclear weapons coming down on Seoul is not worth the liberation the way it would have been before when the only threat they could pose (inaudible) conflict was conventional artillery.

And so I think that these trends in general are requiring us to think more creatively about what is victory and what is defeat, and we're going to have to accept in a lot of these scenarios, well, I hope we don't have to fight any of them, but if we were to accepting partial success may be better than risking nuclear war to try to restore things as they were.

Why don't you comment and then Harlan yourself.

MR. EASTERLING: I was going to say we've already had some previews, I think. You know, Crimea. What was that?

But we elected to stand by and watch and ask what was that? Ukraine. And we're still asking what is that?

It doesn't fit our models. But importantly, it doesn't rise to the level of national importance that I think we'd have to find in order to intervene in some form. What would intervention be? What would intervention seek to accomplish?

The game is changing. Rules aren't as clear, and the tools that are being used.

And then the question was asked earlier about Russian involvement in the U.S. election, a direct outgrowth of the sorts of tools to be used in Crimea and Ukraine and elsewhere, and within Russia itself where (inaudible) seems to be a somewhat flexible subject.

The point about China is very well made. We are not going to become the Pacific hegemony. The point I think the Secretary underscored was to insure that we remain a credible deterrent to whatever behaviors we determine to be against national or world interest. And that's a very important distinction.

For example, there's also a cost imposition which we have successfully imposed against ourselves. Our mode of war is colossally expensive. (inaudible 18:3731) platforms, but at the risk of indicting myself I won't. If you add up the top I think it's 11 now defense programs in acquisition land, you still don't get a 35. Something not quite right when you run programs that are that distorting, and then you look at the capabilities, much debated. I won't do it here. We have 35.
And full disclosure we make about 30 percent of the airplane.

It's a colossally expensive mode of war that we've elected to pursue. The Pacific doesn't (inaudible) that. That situation will not allow us to go forward as we have no matter what the next administration would like to do in terms of forestructure. There has to be a different way of fighting. It isn't as kinetically intensive. It isn't as platform intensive, or certainly platform extensive to the extent that we build submarines where we can only afford three or four, or destroyers such as the Zumwalt where we can only afford three or four. Just doesn't work that way anymore.

So there have to be alternatives, and this gets us back to the technology, no apologies, as well as the organizational constructs for reversing the cost imposition and imposing it upon the opponent (inaudible).

MR. O'HANLON: Thank you. Harlan, do you want to comment? And the we'll go to a final round of questions before we all wrap up.

HARLAN: I'll be exceedingly brief and speak in shorthand. About 20-odd years ago I was part of a group that created shock and awe that was never used by anybody and it should have been because the issue here is how do you affect (inaudible) and perception.

Dealing with China and Russia, what do Xi and what do Putin want its not a war. How do you play to that? China the strategy should not be an air land whatever it's called, air/ sea battle. It should be preventing the Chinese getting out of the first island chain a very, very defensive system that blocks them up which can be affordable, and it's also reminding them that they have about two or three trillion dollars invested in America.

In Russia it's quite the same. NATO has to evolve to the 21st Century, and I've argued for a long time for a porcupine defense rather like the Finnish Winter War of 1939 where the Russian would be bloodied. You see some of this going on in Estonia.

What NATO has to do is be able to provide the counter side with the counter propaganda, the counter intimidation, and quite frankly, we need to talk to the Russians. That's exactly what Putin wants.

So the strategy here is much more than an intellectual one. Knowing what they want, and what we need to get, and then using other means than direct force, but when we do use the military tool, we use it smartly, and as you point out, our cost

exchange ratio is killing us. We're headed to a hollow force in my mind. The fact that we spent 70 billion, that's with a "B," dollars on counter IEDs, and the other side spent pick a small number with 1000 to 1, 5000 to 1 cost exchange.

MR. O'HANLON: Great example.

HARLAN: We have got to reverse that, and that means as Churchill said when you run out of money, you've got to start thinking, and we simply are not thinking. With due credit to the third offset strategy, it's only about protecting the net, not about (blank tape).

MR. O'HANLON: By the way, just one final note, and Kelly, unless you want to add anything here too, and then we'll go to the final questions.

But implicit or explicit in what you said, both of you, was a discussion of economic tools as well as other instruments. And I'd like to see, set up our government in such a way that people who think about war planning actually have experts from Treasury, and Commerce involved, because we had some success in improving the way we apply sanctions. Whether people liked the Iran deal or not, we applied sanctions better to get to the possibility of a deal.

We've got some greater sophistication about how to do these sorts of things, but imagining a multi-iteration, multi- step conflict which is not all military, not all kinetic with a China, or a Russia, is going to be largely an exercise in which economic punitive instruments do you use at which stage, and how resilient are you to the likely responses. And I don't think we're very well set up to do that.

If you ask Pacific Command to do that, they're going to say, okay, send me a couple of economists on detail because I don't really have very many. I've got a couple of people, couple Lt. Colonels who took it a little bit in college and who still like it,

but, as you know better than I, that's not the way these commands are set up, and there's no other part of the U.S. government that's really prepared to do that kind of campaign planning across multiple disciplines and departments.

Did you want to say anything?

MS. MARCHESE: Yes, I would just, I mean, your comment around the, whether the third offset is ever something that we can actually achieve, I think it is the right kind of aspirations just the degree to which we can expect to get to, but I think it's an important aspiration.

And on the economic side, every investment needs to be prioritized, and if the third offset is not entirely about the technology, but that's where all of the resources are being spent, the differentiation can be about the visibility and the agility and the creativity to be able to respond to different situations that are out there. They're not all going to look like they have in the past.

MR. O'HANLON: So let's take that final round of questions, and then we'll do the final round of responses. And I think I saw two or three hands, or, actually, okay, I see four hands, so we'll do two rounds of two each starting here in the front, and then with the gentleman in the black jacket, yeah, here in the front with the bow tie, I think.

And then that'll be this first round. And then the second round would be Greg and Brendon.

VOICE: One of the reasons why the Soviet Union for 70 years without being very innovative, you know, was that they were innovative in the field of spying so they would get your secrets on the cheap including the Manhattan Project. And today we can see that China is doing a similar way of thinking because it seems that their liberation

the last 20 years have had some similarities with the new economic policy from Russia in the 30s where they got a lot of American technology.

Last three years with a new dictator, it seems that China is (inaudible) down their way of exchanging information me it more difficult for U.S. to understand what really is going on in China because they following the teaching of Ivan Loch, "The Future of War," which is not much read in the west.

MR. O'HANLON: Thank you. And then the gentleman back in the red tie. Then we'll have responses.

MR. BOOKER: Hi, Ben Booker from the Reserve Officers Association. So we talked a lot about like the technology, the hardware, the organizational aspect. I wanted to kind of touch on some of maybe the personnel questions.

So Defense Secretary Ash Carter has talked about the Force of Future Initiative about looking to see how he can make personnel policies more flexible to allow for these creative, like people that have the agility to master these technologies to come into force. Public-private partnership were mentioned as well. So just coming from my perspective as somebody who works with Reserve and National Guard forces, do you see a role for the Reserve and National Guards in helping link these public/private partnerships and allowing for this greater flexibility, agility to master this technology like you said that's coming more from the commercial space where maybe Reservists and National Guard members have exposure to as opposed to a active duty personnel member?

MR. O'HANLON: You want to take that latter one

and --

MS. MARCHESE: Yes, sure. So I think the talent implications of where we're at right now are fascinating. We were talking about that before because we are in short supply of great talent, and so how do we attract the great talent that has the interesting level of expertise on the technology side, and the innovation that had the desire to serve.

And so I think the Reserves would be a great intersection there. I hadn't thought about that before, but I think that's really important.

We've got to get more of our talent up to speed, focus a lot more on the stem side than we ever have before in order to grow that talent, but also at the same time attract some of the best talent that are going into other industries. right now.

MR. O'HANLON: Alan.

MR. EASTERLING: It's a great question. And I'll stick with the talent for a moment. To elaborate on the earlier discussion that Kelly and I were having, there's a global technosphere, as I alluded earlier, which is being fueled by human capital on the global scale. And I love the Bill Gates observation that if you're going to be one in a million in China, there are 100,000 just like you. That's the implication of the technosphere.

We like to think at Northrop Grumman that we're this very attractive employer, we are, to whom this sort of talent would like to come to work. Sometimes is the answer.

If I go to MIT, and I walk into the (inaudible) Department, they know me. And they don't know from Grumman, and they want to come work for us and they do. Thank goodness, right?

If I go to the next building over to COMSCI, Computer Science, they've never heard of me. Now, the U.S. Army walks in and says I'm hiring people, well, you know, and yet that's exactly what has to happen, right? The type of technology that we're talking about, and by extension the type of warfare that we're talking about requires people with these extremely in demand skills.

Now, the speed of commercial technologies have been that we've not talked about, right? But we're developing a number of leading-edge technologies in the computer world I won't go into here, but we have concern about the protection of intellectual property. And in conversation with a mature computer industry, they say what are you talking about.

Well, we'd like to patent this and trademark that, and they say, no. The way you protect IP in this world is by going faster than anybody else.

Now, for anyone with experience in the defense acquisition system, does that sound like defense acquisition? So you've got two threads here, right, the technology thread and the human capital thread which are coupled running out ahead of us even as we sit here and say I need all of that in order to build this third offset construct hypothesized.

The short answer to your question is it's possible that a reserve component might be the way to tap into that.

VOICE: I'll just say a brief work on the spying, the we'll go the final round.

I think that you're absolutely right that we have an ongoing big problem. President Xi has promised to try to stem some of the intellectual property theft. It remains to be seen if that's carried through upon.

I would think it would not be for the kind of technologies that we're talking about because even if there are commercial standards that we think we can pressure China to comply with if they want access to our market over the long term.

In the defense sphere, this step is legitimate espionage at least by our traditional definition, and we would certainly look to learn about any kind of the equivalent of a B-21 being built by China if they were sloppy enough to, not the north that was supply, but our government as sloppy, and lets these kinds of secrets be accessible through some kind of means.

So if what you're talking about is protecting military technology and the Chinese can be persuaded to behave by different standards, I think the answer is going to be no. In fact, the OPM, you know, theft of the 21 million, you have to view that as basically sloppy American protection not unexpected Chinese behavior.

And even though in theory an F-35, or a B-21, or whatever is a commercial investment from a state-on-state perspective, it is a national security asset, and therefore it is fair game for espionage.

I'm not trying to endorse that, but that is going to be how spy agencies around the world will look at the situation.

MR. EASTERLING: If I may --

MR. O'HANLON: So please. I actually want your response on this, but I would simply say in the commercial area I think we can think harder about using punitive sanctions, and in the investment areas, I think we have to work very hard to question if we're letting Chinese companies, especially state owned companies, buy too much in the way of American technology assets, but in the classic espionage realm, I think we're

going to have to view this as natural state behavior and just get better at protecting key secrets.

MR. EASTERLING: And I completely agree. I was only going to add that I had the honor of having the same discussion with General Michael Hayden earlier this summer, and he said essentially the same thing. These are legitimate targets. This is legitimate statecraft. And in terms of European breach he said if I could have done it (inaudible), I would have.

MR. O'HANLON: Interesting.

MR. EASTERLING: Yeah.

MR. O'HANLON: So we have two last questions for my two friends here in the middle, and then we'll wrap up.

VOICE: Hi. Greg (inaudible) with U.S. Steel. Couple things that you addressed earlier which kind of all kind tied together.

Michael, you mentioned the ICBMs, and we talked about the lack of connectivity which was not by design but just by an outdated system.

And then, Alan, you talked about some of the MCON operations and how those would apply here. For the past 30 years every since the end of the Cold War, we've been operating essentially in an unopposed environment where were can rely on these network systems and be able to execute without any problem. Now, we're seeing some threats that may take those down.

So the question I have is as Harlan talked about some of those cost imposing strategies or in our case the inverse cost imposing strategies, do we throw more solutions at the cyber problem to create better defenses and more resilient networks, or are we going to fall back to a more autonomous type of operation where

we're looking at MCON like operations where we send out small units that are assigned a mission and they're cleared to go and execute those missions without having the generals and admirals watching from the (inaudible) as they go through a targeting process, or is there a balance between those two?

MR. O'HANLON: Thank you. And Brendon, last question.

MR. MARINO: Bernie Marino previously with the defense team here at Brookings. I think partly in response to Sidney's question, Secretary Work mentioned that Americans as opposed to operators from authoritarian regimes are best positioned to use connected technologies and networks.

I've also heard him say publicly elsewhere that in cases where those networks that are taken down or otherwise manipulated, Americans are also best advantaged to respond to that, and I'm wondering to what extent do you think that's actually the case?

MR. O'HANLON: Alan, do you want to start this time and then Kelly can finish up.

MR. EASTERLING: Yeah. Both great questions. So most of you will be familiar I imagine with Tyler Cohen (inaudible) Nation. Wrote a wonderful book on some of these questions from an economic standpoint.

And he writes about what I've heard Secretary Work call Centaurs. He doesn't use that term, but it's the human/ machine teaming that we'll get into.

And the observation has been made that after Kasparov finally fell to computer, a new form of chess evolved called hybrid chest in which human and machine teams, and this is usually two or three people working with a chess computer or algorithm, competing against another team of two or three humans and the computer.

And the humans are maintaining the strategic perspective, the big picture on the board. And the machine is running through the millions of moves or communitorial scenarios that might come out of the strategy.

And what's interesting about this is the hybrid team will defeat any computer made and, of course, any human. And it's a wonderful way of illustrating the synergies between the AI that we have in mind and the humans I think in a simplistic way, but also highlighting the inherent superiority of the cultural and societal aspects that we bring to war. We tend to be very innovative people. Autocratic regimes tend to struggle with that, and I think that the Secretary was hinting at that. They prefer the automatic mode. Quite a centralized road,

And so you take that sort of thing out of it.

Well, I joked earlier about the highly chaotic nature of war, it is. It's not a joke. And that innovation and adaptability is absolutely essential, I think.

I don't care how sophisticated our learning machines become, they're going to have difficulty contending with all aspects of the battle space in a way that humans have proven rather good at.

And I believed that the two combined and the mode of combination, and, of course, it domain dependent, right, is what will set us apart from our adversaries who may be more inclined from a cultural perspective or other consideration to fall back on the more automated side.

Speed of war will always be a question there. Machines will always react, think, decide, plan, replan faster than humans. And we haven't spent much time talking about technology such as SUMS. Secretary Work has talked about that. Northrop Grumman is all about unmanned, but the most sophisticated unmanned

systems in the air today are essentially conventional aircraft with very good auto pilots. And they tend to operate as individual units. What we and many others are looking at doing is how do they perform as a kind of, sorry to go Terminator on you here, but how do they perform as a kind of super organism, and that's where we get the term, swarms. We observe swarms in nature, ants, termites, bees, humans actually demonstrate swarming behavior.

And then you pit swarms against swarm. And the science fiction genre is filled with examples of this sort of an enders game, the most recent Star Trek, you know. That's where all of this winds up taking you. But you never take out the human piece, and you have to draw from the strength of your inherent culture, and I think that that renders us with an enduring advantage.

MR. O'HANLON: Great.

MS. MARCHESE: And I agree with that. You never take the human completely out of it. They have to have a new and different role, and we've seen humans go from having to use an advocacy, and now nobody uses that. So they have to have -- the way businesses operate, networks operate, there is so much complexity, there's such a massive amount of information you have to have the machines have that role, and then the human side of it takes on and makes some of the more complex decisions with all of those insights that are brought to it.

MR. O'HANLON: Well, listen. Thank you all for being here, and please join me in thanking the panelists. (Applause).

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020