Admiral Mike Rogers (Ret)
Former NSA Director and U.S. Cyber Command Chief
Senior Advisor, Brunswick Group

Suzanne Spaulding
Former Under Secretary of the Department of Homeland Security
[Cybersecurity and Infrastructure Security Agency]
Center for Strategic and International Studies

Frank Sesno - Moderator

How Should the Biden Administration Tackle the Cybersecurity Challenge?

Defense Writers Group
Project for Media and National Security
George Washington School of Media and Public Affairs

12 January 2021

DWG: Ladies and gentlemen, welcome to this conversation on the cybersecurity challenges faced by the incoming Biden administration and how it should tackle them. This session is cosponsored by the George Washington University Project for Media and National Security and the Howard Baker Forum. I'm David Ensor, Director of the GW project which is part of the GW School of Media and Public Affairs.

This conversation comes, needless to say, at an extraordinary time in our nation's history. We'll have a new President taking office next week. Last week a mob attacked Capitol Hill after President Trump urged them on. The House is considering impeaching Trump, but even before that there was the Solar Wind hack which U.S. intelligence agencies have now said they believe was conducted by the Russians and it clearly has wide and serious implications, many of which we don't know enough about yet.

So as we look to the next administration's approach on cybersecurity there's much to discuss and I'm thrilled that Frank Sesno, a former CNN broadcaster, a friend, and a colleague at GW will be our moderator today. He's going to introduce our two distinguished guests and after asking each a few questions himself he'll recognize those of you who'd like to ask a question as well, at least as many as we have time for.

Frank, over to you, sir.

Moderator: David, thank you very much. As you say, this is an extraordinary time in this country. It's an extraordinary time to have a conversation like this. I'm delighted to be part of it.

Let me say at the outset that if you do have questions what I hope to be able to do is have those of you raise your hand as we're wont to do in Zooms and if you're on camera, I will come to you. Right now. And this is a note to Chloe who's working in the Teams and listening in, I'm not seeing everybody who's involved in this event. I'm seeing more on the participant list. So perhaps that's something we can work on. If I can't get to you with the camera you can certainly submit your question in writing in he chat and I will pass that on.

We're joined by two remarkable people who have a very knowledgeable and unique perspective on the cyber challenges that we face and other challenges that we face in this country right now which are many. Admiral Michael Rogers, former Director of the National Security Agency, former Commander of U.S. Cyber Command. He's now a Senior Advisor to the Brunswick Group. And even though I am wont when I hang out with admirals, which isn't very often, to call them Admiral, he's insisted I call him Mike. So I think that disclaimer is important up front. So Mike, thank you for being here.

Rogers: Thank you.

Moderator: Also Suzanne Spaulding. Suzanne Spaulding is the former Under Secretary of the Department of Homeland Security. She's now a Senior Advisor for Homeland Security with the Center for Strategic and International Studies. Suzanne, if it's okay, I'll call you Suzanne. You call me Frank, and we'll all be on a first name basis.

Spaulding: I love it.

Moderator: Great.

What we'll do is we'll have a conversation here. I'd like to start with Solar Winds for sure and then broaden to some other things and then open it to the questions from this group of journalists and others who are very knowledgeable in what is going on and probably have some very specific and certainly very

informed questions.

There can be no question that the Solar Winds hack is an abject disaster. Even more is the complete misread of the cyber battlefield it would seem.

Reuters had a story not too long ago that at a dinner General Paul Nakasone, who is the head of the National Security Agency, U.S. Cyber Command, in late February said that ''U.S. teams were understanding the adversary better than the adversary understands themselves.'' Well, not true unfortunately and we can see what's happened.

Let me start by asking each of you, and Mike maybe you'd like to go first, based on everything you now know, much of which has been provided by the journalists here presumably about the Solar Winds hack, what worries you most?

Rogers: I would argue, number one, that the fundamental structure we have put in place is not optimized to the challenges of today and tomorrow in many ways. It doesn't mean that they're not hard working and motivated men and women, I don't mean to imply that. But we have focused on collaboration where I think the answer is integration, and I just think collaboration doesn't take it far enough.

And secondly, we have historically highlighted three types of behavior in cyber as unacceptable. We have said the theft of intellectual property, whether it be by a criminal company, industrial competitor, or a nation state, is unacceptable. We have said the penetration of systems via cyber, systems associated with the safety, the health and the well-being of our citizens and the critical infrastructure associated with the uniqueness of our nation and our economy, that that's not acceptable. And we have said that criminal behavior -- ransomware, extortion, et cetera -- is unacceptable.

What we have never said as policy across multiple administrations is the penetration of national security systems during espionage purposes is outside the acceptable [means], and one of the challenges I think for the incoming Biden team is we need to step back and ask ourselves, just what kind of behavior is unacceptable? And if so, what are things that we can use, if you will, to kind of set thresholds, so to speak.

Moderator: I think that's important to lay that out.

Spaulding: Great, Mike. I do think on your last point that before we start issuing kind of red lines or what's acceptable or unacceptable, that we need that second part that you articulated which is we need to then have a clear plan for what we're going to do when those lines are crossed because there will be efforts and we have to assume that those lines will be crossed.

Part of that means we have to continue to work hard to develop the tools that we need to be able to have an appropriately calibrated response. One of my concerns has always been that we kind of have the nuclear option or nothing, and very little that -- we need to be able to turn the rheostat, turn the dial to have responses that are meaningful and appropriate and proportionate to what we're seeing.

I think my greatest concern, your question about this massive hack, is that we for some time now are going to have to assume in government and certainly in many of these private sector industries that have been impacted, that the adversary's in our system. That the adversary is there. That we are going to be a long time getting that adversary out of our system.

As Mike can tell you, his folks know very well, Rick Ledgett has talked about these. These factors, when you discover them in your system they don't just melt away. They do hand to hand combat. Our folks are going to be fighting them for quite some time and then working to rebuild more securely and even at that point again, we have to -- we've talked about it forever, but we have to really operate on the assumption that bad actors are going to get into our system. Now plan accordingly.

That's really hard. I've talked for over a decade now about the need to train to fight in the light. Train to fight in the dark. You can turn off the lights and meet your adversary at night or in the dark and have the advantage. We need to recognize that the shelf life of secrets and our ability to keep adversaries out of our systems is vanishingly short and we need to train to operate in these potentially degraded environments and learn to operate with fewer secrets, et cetera. But that's hard.

Rogers: Think about it. This was a high end actor, among the most capable in the world, who sustained access for at least nine months without any external awareness. And as an individual,

among others, who both penetrated and defended systems for a living, in nine months what you can do in terms of assuming new identity, changing system configuration, creating alternative access. I'm like look, the idea -- to Suzanne's point -- that this is a short term issue, we'll drive them out. Boy, this is a long term sustainable effort.

Moderator: And I want to come to some of the change and reorganization that is likely to be done and confronted by the Biden administration. But before we do that, I want to stay on Solar Winds for a couple of minutes and a couple of questions here.

One of the questions raised, and it's a very big one with this one, is did the hackers have the ability merely to observe communications and do sort of espionage or was it much more than that? Could they compromise systems? Could they influence or disrupt operations, destroy systems?

From what you both know and have heard, does Solar Winds go beyond mere intelligence gathering?

Spaulding: First I would sort of push back a little bit, Frank, on your use of mere.

Moderator: I'm being sarcastic there.

Spaulding: But I think the connection, you understand it and folks on this call probably do, but a lot of people don't appreciate the connection between reconnaissance, gathering of information, and the ability to have an attack that has an impact on the physical world. Right?

So we always are, did they breach operational systems? Did they get into a [inaudible] and host systems? If not, whew, we're good to go. And the flip side of that is, oh, if they got into an industrial control system they can take down the electric grid tomorrow.

And of course the reality is that you need both. You need that reconnaissance in order to have, to be able to threaten, which is my greatest worry, threaten to have an impact on critical infrastructure or have an impact. You need to have both the access to those industrial control systems and the detailed knowledge of the operational processes that they control so that

you can figure out what actions you can take to have the greatest impact.

So my worry is we don't have an indication yet that they got into operational technology, that they got into industrial control systems with this attack, with this particular campaign. But I am worried about whether they were using this in part to gather information that will help them if they already have access to places or future access [inaudible].

Rogers: For me, I would say number one, we don't know enough yet to make a definitive statement. The reality is we need greater understanding of just what happened and that understanding is likely to unfold over the coming weeks and months. Not days.

The second point I would make is what always worried me the most was not just extraction of information. I worried about manipulation of data, degradation or manipulation of system configurations, and thirdly, activities associated or lay the basis for future options down the road. That's what Suzanne was talking about.

The biggest concern I have here and one that I'd like to see some public comment on was, was this activity confined to just the unclassified aspects of government infrastructure or were there classified implications? And let me be very honest, I'm not pretending that I know that. But having been on the other side, as Suzanne has been, one of the first things I was always talking to decisionmakers about was, are we confident that we understood who this actor is, what they did, how they did it, what their intent was, and that they went no further? And I just don't think we're in a position to answer those questions yet.

Moderator: Suzanne, you agree with that? We can't answer those questions yet but those are the --

Spaulding: Yeah. There have been some public statements, I believe, saying that since they don't have any indication that any classified systems were breached, so --

Moderator: Are you comfortable with that?

Spaulding: I certainly would like to think that that is an accurate statement that reflects their knowledge to date. And I think Mike's point is, we can't know that they know everything

yet, right? So we should expect other shoes to drop. Whether that will be one of the shoes or nor, I don't know. Those systems are very well protected. I don't think we should assume they've been, I mean I do wonder whether folks on the inside shouldn't assume they've been penetrated, but I don't think we should assume that they have been penetrated. But Mike is right, we won't know for some time I think definitively.

Moderator: Senator Dick Durbin called the Solar Winds hack virtually a declaration of war. His words. Given that, and it's a very serious assessment obviously, but in any case what is your take on what the Biden administration's likely legal and policy context is going to be going forward?

Spaulding: With respect to the Biden administration on cybersecurity, I think we've seen some very clear signals right off the bag. We've had cybersecurity mentioned by President-elect Biden on numerous occasions which is something that a lot of public officials never use that word and never talk about that subject. He has given remarks specifically on Solar Winds and on our cybersecurity posture. So right off the bat we know this is going to be a priority for the President.

He has chosen a team of people who Mike and I worked with in the last administration, in the Obama administration, who lived through things like the OPM hack and other major cyber incidents who are very familiar with the consequences of insufficient attention being paid and so for whom this will be a very high priority.

Right off the bat I think we know this is going to get senior level attention and across important departments and agencies, all of which need to be focused.

Rogers: I would agree with that. As Suzanne said, we both spent years working with these teammates, so I won't speak for Suzanne but as I look at it, it's great to see good people, motivated, capable, very focused, and a leadership clearly that is articulating this is important, we realize it's important and we're committed to addressing the challenges. Even if we don't have all the immediate solutions to these challenges.

What I would try to say is number one, we need to think before we act here. We're going to set some important precedents, particularly because this type of espionage or national security

activity as I said before is not something that we historically had defined as unacceptable or outside the acceptable norms of behavior. So we need to think our way through that.

I also think we need to put a lot of time into getting the basic structure right. I was part of both the Obama team and the Trump team. I thought the Trump team, I thought they did well in terms of operational ideas in cyber. Where I thought they were not as strong as we needed to be was prioritization of cyber and the structure associated with cyber. I just thought we didn't really deliver what we needed to. So those are areas where I would suggest for the Biden team, there are some good places to start.

Moderator: Let's talk about structure for a minute and let me just observe that the journalists who are joining us today have written about this and know a lot about this and perhaps I can ask you to go into some particulars and specifics because it's a very knowledgeable group we've got here. The administration's going to have to decide which agencies are responsible for what, obviously. Presidential Policy Directive 41 outlines steps for federal cyber incident response.

So in your view, and Mike obviously you've got views on this; Suzanne, you've obviously got views on this. What role should DoD and others going forward, how should the new administration structure the most effective cyber team and command that it can put together in light of what we now know is going on?

Rogers: First, we have a couple of aspects with structure. We need to address the policy implications of cyber and we need to address the operational aspects, the nitty-gritty of actually defending, securing and ensuring resilience.

I would not use the sane structure to be both. One of the things experience in DoD teaches you, and it may be flawed but it certainly after 37 years in uniform there's a reason in DoD why we tend to separate policy and operations. We don't create organizations and structures that try to do both. They interrelate with each other but we've got to clearly define policy framework structure and clearly define operational framework structure. I would argue that should be applicable in cyber.

We clearly need to make sure that cyber has both prioritization as well as the ability to actually reach key decisionmakers.

I thought one of the challenges of the last few years was we embedded cyber so low within this hierarchal structure that quite frankly trying to get to the senior-most decisionmakers at times to actually execute whether it be policy or operations was more challenging than I thought it should have been, which I think we need to overcome.

Lastly, and Suzanne will want to chime in. The biggest change that I would argue, and I alluded to this a little in my opening remarks, I was always struck by the idea that if you look at our closest partners, the Five Eyes, all five of us looked at cyber. Four of us came to the conclusion that to develop capacity within the government we needed to bring together capacity across cabinet or departmental lines. Only the U.S. really came to the conclusion the answer is we're not going to really integrate DoD, intelligence, law enforcement. We're going to create separate structures and then they're going to collaborate together. I would argue that the last 15 years demonstrates that is not an optimal approach to what we need to do in cyber, either from operations or from policy.

Spaulding: This is one area where I think Mike and I don't agree. I don't know that he'd go so far as to call for a Department of Cybersecurity, but certainly others have. And I really do think one of the things -- we learn wonderful lessons from our allies and particularly from our Five Eye partners, but it's important to remember that the other four are much smaller governments than our government is, and you could argue that I suppose goes either way, but I really do firmly believe that we can't pretend that this isn't a mission area and a challenge that requires all the departments and agencies really to have some ownership on addressing this challenge and that there are certain key elements of our government that have to have major roles in this and they need to be embedded within, they need to have the authorities, the capabilities, the resources of their communities. So we need a strong intelligence component to this that has unique authority and reach back into the intelligence community.

So for example, one of the things I took from Solar Winds is that we still are looking where the noise is. We are looking for our car keys under the street lamp because that's where the light is. We are not, still, as far as I can tell, taking the kind of strategic look and understanding that this, we say a Russia

problem, a China problem. So as we're thinking about our cybersecurity posture vis-à-vis our adversaries, we need to put it in that broader context. That's the reach back to the intelligence community and the Russia experts, for example. So I think that's critically important.

On the issues that I worried about on a daily basis at DHS around critical infrastructure, I was so pleased that Congress accepted our strong recommendation and proposal that CISA not be just cyber. That it continue to be physical and cyber, all-threat approach to that critical infrastructure. That convergence is critically important for understanding the threat, assessing the consequences which have to be a hue part of prioritizing your allocation of resources, and that comes from understanding those businesses, those operational processes, where they fit in, et cetera. Not just their network. But also in mitigation. The way to buy down risk, to reduce the risk from cyber may not be just in your IT defense and systems or even in the deterrence effort. It might be building your resilience against the consequences in the real world. Putting in hand [cranks], having paper ballots. And I worry that if you just pull all the cyber pieces together, it becomes all about the technology. We saw this with WMD. You lose the strategic look at what countries' strategic objectives are and how cyber fit int, so where we ought to expect to see them, not just where we do see them. You lose that sense of what we really care about which isn't the computers, it's what the computers enable. Right?

So I think it's really important that it has to stay distributed. DOE has to have a key role. Department of Treasury for finance, et cetera.

Which means -- sorry to be so long-winded -- that you do need that central, strong coordination at the White House, and as a member of the Cyberspace Solarium Commission of course we recommended the National Cybersecurity Director.

Moderator: Mike, respond to that and address the role of CISA in the Biden administration.

Rogers: I don't intellectually disagree with the idea. My only point would be we didn't resource it to execute that spectrum of missions, number one.

Number two, I think part of the challenge in this, we have to

acknowledge for right now, and hopefully this will change over time, but we are today and are likely to be at least for the immediate future, to be in an environment in which there's not enough resources and not enough expertise to go around. So this idea that we're going to make every separate organization create their own structures, I just think we don't have the resource capacity. Don't worry about the money to acquire it, I mean literally we don't have enough people and enough expertise to really do that. I just think the future at least in the near term is much more about integration. It was never about, my attitude about it as a uniformed, as a military guy was this shouldn't be about DoD or Intel being in control. Heck no. We should be an integrated part of a broader team.

I like the idea that DHS in its broader role -- cyber was a key element. I always thought that was a strength. My only frustration was why are we trying to do this with just one under-sourced organization and one cabinet segment assuming overall responsibility. I just don't think this is going to work in execution. It also goes to Suzanne's point about when you're focused on the day to day operational piece it tends to drive you down into focusing on what you're seeing on the [noise]. It's another reason why I never liked policy and operations being in the same organization. I thought we wat to separate that perspective. We want an element that's focused much more on the long term and the core strategic implications of this separate from who's rolling up their sleeves trying to deal with the day to day? And both of those functions are incredibly challenging.

Moderator: Let me ask a little bit about operations. Where we've been and where we're going in the context of persistent engagement.

This is predicated on the whole notion that everywhere is next. Front line's all around us. And you're persistently in contact with the adversary, the enemy, right? It's supposed to be ongoing, constant confrontation, probing, learning, supposed to provide insight, intel on what's going on on the other side. What's the capacity.

So with respect to Solar Winds, was persistent engagement just a massive intelligence failure not to know? Did persistent engagement itself somehow fail or the implications of that?

Rogers: For me, my first comment is we're mixing apples and

oranges. To me. You take it for what it's worth.

First I would say we set as a goal and we used persistent engagement as an element of a broader strategy with respect to Russian interference int eh 2018 elections via cyber. Russian interference in the 2020 elections via cyber. That seemed to turn out very well. I don't draw the conclusion, therefore, that it means the strategy's perfect, nor do I draw the conclusion because of Solar Winds the strategy is inherently flawed.

I think the challenge with Solar Winds goes to again this idea of does Solar Winds represent activity that is unacceptable? And if so, how do we define it? And what kind of policy, to include persistent engagement in other elements of the strategy. Remember, persistent engagement is highlighted with Suzanne and the rest of the team on the Solarium Commission, they did some great work. They highlight the idea of defend forward and persistent engagement as elements of something broader and that you can't just view one element of that broader strategy as that's the cornerstone, that's all we need to focus on. Or conversely, if something failed it was that one key component. I just think we're drawing the wrong lessons here. I just think we need to step back and look at this a little bit more broadly.

Spaulding: I agree with Mike. We run the risk of learning the wrong lessons and not understanding that we need to be able to walk and chew gum at the same time, and that there are all elements of what the Cybersecurity Solarium Commission called a layered strategy.

So persistent engagement has got to be a piece of that. If anybody thinks that's all we need to do and we're done, we're persistently engaged, we're creating friction, we're good to go, nobody thought that. And this is why one of the most, the pillars that we emphasized I our report was resilience. We've always said you should assume you're going to do everything you can do. All of the things we talk about to deter the adversary through diplomatic norms and signaling and that persistent friction, et cetera. Everything we can do to defend our networks. The perimeter, the inside of the networks, all of that stuff. Then we have to assume that they're going to overcome all of that. That they're going to ignore our signaling and our deterrent efforts, that they're going to overcome our defensive efforts, and they're going to penetrate our system. Now what's our plan? Right? That is risk management. That is what I

preached for all those years I was at [NPD] to our private sector folks and my government partners. What are your mission essential functions? To the extent they're dependent on cyber, assume that's going to be a vector for disruption. Now how are you going to mitigate that potential impact? What are you going to do now?

Rogers: Can I make one other comment about Solar Winds? I think it also showed you how adaptive adversaries are in cyber. It was a supply chain attack which we have seen executed previously in 2017, NotPetya, the Russian effort against the Ukraine. Hey, they used a supply chain vector as the primary.

What's interesting to me, if you look at the difference between the activity we saw in Solar Winds and [inaudible] areas, one of the thigs that struck me was the Russians shifted from a focus on using infrastructure outside the United States and they tried to hide within the noise within the domestic infrastructure. That's important to me because much of our -- I'll only speak for the intelligence in the defense world, much of our focus, much of our authority is all predicated on external, foreign. And yet I'm watching an actor who clearly saw that. They knew -- one of the reasons why we were able to generate such significant insights on their actions in 2016 was because we had a sense for how they operated. They have clearly pivoted into a different operational scheme, a different operational methodology and they're using our structures and our processes in some ways against us. We need to be thinking our way through what are the implications in that.

Spaulding: It's interesting, Mike, because they made the same pivot in the disinformation world.

Rogers: I agree.

Spaulding: To amplifying domestic voices in the hopes of really complicating our response.

Moderator: And maybe they succeeded at that.

I'm going to ask one more question here and then I'm going to open it up to questions from the journalists and others who are joining us.

Let me ask you both this. The terrible disturbances that we have seen, the insurrection on Capitol Hill, the concern about

violence and perhaps unrest in state capitols literally across the country over the coming days. What does this suggest to you about the cybersecurity landscape that we're confronting? What's the correlation, if you think that there is one, between the domestic unrest and riots that we have seen and what's out there in the cyber world?

Rogers: I think from my perspective you clearly saw, it was relatively minor but I think you saw a cyber element of the activity on Capitol Hill on the 6th of January. There are reports of theft of laptops, theft of cyber-associated physical infrastructure since they penetrated physically the spaces in the capitol.

From a cyber perspective what really concerns me and I think it is only a matter of time, the when, not the if. I think you're going to see a cyber dimension to domestic unrest. We've seen it manifest itself largely in the physical domain. Rioting, protests, marches. I think that you're also going to see over time a cyber -- you're already seeing an informational aspect to it. I think you're going to see a cyber dimension.

Moderator: What would that look like?

Rogers: I would not be surprised, in fact I'm doing some things with at least one state where I said look, we need to think about the domestic piece in cyber. We've so optimized ourself for the foreign piece, we haven't spent much time thinking about the domestic piece.

So you will likely see I my opinion over time people using the ability to penetrate cyber system, to deface web sites associated with particular movements, to try to knock off-line the cyber capabilities of government organizations. To attempt to use cyber as a tool to inhibit police and security forces' ability to respond to demonstration.

You look, just in the physical domain. You look at the weapons and the capabilities that were within that set of people on Capitol Hill on the 6th of January, this wasn't just -- not that it's true of everyone but there was clearly an element there that thought we're going to bring a wide range of tools to help us maximize the damage and the effect of physically penetrating the capitol.

Moderator: The worst case scenario. The one scenario would be these kinds of attacks literally in 50 states across the country. Who tracks that? Who monitors that? Who's got the capacity for that now?

Rogers: Right now clearly that's a law enforcement, DHS and CISA are focused on a component of this. But what this unrest shows you is broadly we had not prioritized, and I'm not trying to second-guess anybody because there's not enough resources to go around. But we probably I think it's fair to say have underestimated both the level of unrest, the organization within that unrest. There is a level at least in some components of clear organization. The level of capabilities that some of these groups and individuals are able to bring and that I look for that to expand into cyber and other areas. I just think this is a focus -- we've got to think about this in a way we haven't before.

And again, much of our government capacity -- and I say this as the individual who was part of the largest intelligence organization in the U.S. government. We are totally by law and by cultural norms focused on we're a foreign intelligence organization. And yet we're finding ourselves as a society dealing with a set of internal challenges we haven't seen in a long time.

I am not arguing the answer is we'll turn the federal government loose on the domestic environment. That is not what I'm saying. But what I am saying is we need to step back and have a conscious discussion as a society and as a government about what should the role of government capability to understand this dynamic be? How should they be used? How should they be controlled? What level of oversight and protection should we put in place? But we can't sit here and say I don't think this is something we need to eb concerned about.

Spaulding: Of course it's nothing new. We haven't used the term in a long time, but hactivist. This is not the first time that we have had to think about political activists using cyber, certainly for the kinds of things Mike talked about in terms of web defacements and that kind of thing.

This may be more domestic origin, though some of that was I think as well. So we need to not forget our lessons from the past.

One of the things that I do think -- Mike also mentioned the prospect for disruption and I do worry a lot about that. I am very worried about, for example, the prospect of disrupting communications between our deployed forces around some of these key dates and potential events coming up. That would certainly be a way of using cyber to have consequences in the real world, to frustrate our ability for a variety of deployed federal forces to communicate and coordinate with each other.

But one of the things I think is interesting is we have hactivists on both sides of this and we may be already seeing some of the battle between the ideological spectrum here. Somebody mentioned to me today that it looked like Oathkeepers' web site was down. That could be for any number of reasons. Who knows? But my first thought was, somebody who doesn't like what they're doing is using their cyber skills to go after them, so we may see some of that as well.

Rogers: I think bottom line, cyber becomes an extension of what we're seeing in the physical --

Moderator: Let me turn to a question from the audience. This is one coming through the chat.

A question for Admiral Rogers. What effects do you assess will come from eliminating the social media presences for Donald Trump as well as for those who have planned and coordinated violence and deadly protests in recent days? Do you expect this will succeed limiting the organization of similar violence in the future? And are there any dangerous precedents here?

Rogers: I don't think there's any one step that collectively we're going to take that we're going to be able to guarantee that it will stop the spread of violence. I just don't think that's [inaudible].

I do think that in the midst of all of this we do need to be mindful about at its core what makes America what it is. And just as in the aftermath of 9/11. When you see traumatic events that create a visceral, real, raw emotion, where we see people's lives being lost, where we see symbols that mean something to us whether it's a skyscraper in New York or the Pentagon, for example, on the 11th of September. Those produce visceral human responses and the reaction is often in a very human way, I want to make them pay. I want to make sure that never stops. Those

aren't bad reactions. The challenge has to be but in so responding don't forget who we are and what we are.

For me at least, I don't want to compromise who we are and what we are as a nation in the name of our security or in the name of vengeance or accountability. And those are two very different terms, very different meanings. One generally considered positive, the other somewhat negative. But we need to step back and think about what we're doing before we just man, I am unhappy, I am frustrated, I am pissed off, and by God I'm going to do something about it. Let's take a deep breath and think our way through this before we just act because we're setting important precedents.

Spaulding: Mike is right. I spent three years looking at the ways in which Russia has used information operations to undermine public confidence in our justice system, exacerbating preexisting wounds and grievances. And one of the things I've said, and I think it's true of many of these domestic actors on-line as well, is that they are trying to practice jujitsu. They are trying to use our strengths against us. And I think we need to remember that those are strengths. Those are our strengths and not to throw them out. Not to let our adversaries and bad actors cause us to unilaterally disarm in the information space.

So I think Mike's caution is very well taken.

Having said that, I do think that clearly, first of all a lot of Americans don't understand, the platforms are not governed by the First Amendment legally, from a legal standpoint. That only applies to the government. But we do want to uphold the principles that underly that and the value of a robust marketplace of ideas. So uncomfortable speech, speech with which we disagree, et cetera, we have to be very careful about the ways in which we weaken ourselves by blocking that.

But that's different, I think, from unlawful activity and inciting and planning and coordinating violent activity and unlawful activity. And I do think that the platforms, they have liability protection because we want them to moderate that kind of content. So they need to step up and do that.

There's a lot of talk right now about how much power these platforms have and are we in fact silencing people when we shut down their accounts or we shut down other platforms effectively

by denying them access to app stores and that kind of thing.

I do think we need to continue to look at the power of a handful of platforms and I think lots of interesting and creative suggestions out there including promoting more competition by forcing interoperability among platforms. Those kinds of things need to be seriously considered and looked at.

Moderator: I see that Kimberly Underwood has her virtual hand up.

DWG: Thank you, Mr. Sesno, and Professor Ensor and Admiral Rogers and Admiral Rogers and Under Secretary Spaulding for your time today and for this great event.

I'd love to get your take on what you think is needed at the State Department in terms of international cyber policy. I know the Cybersecurity Solarium has called for a more holistic strategy and then there was action by the Trump administration to create a Bureau of Cybersecurity and Emerging Technology. What is needed from that kind of perspective for that specific department?

Spaulding: The Solarium recommended the creation of a Bureau for Cybersecurity at a very senior level. I think we said at the Assistant Secretary level, but I'd have to go back and look at the specific recommendation to confirm that. But our thought was this needs to be given priority in the State Department and placed at a senior level, and it needs to be empowered by the Secretary of State and by the White House. And it needs to take on a number of tests. Not just coordinating efforts across the government to work with our allies, our partners and allies on collaborative efforts, whether that is efforts to build a more robust supply chain or develop norms, but also to have a much more strategic and robust presence and standards body.

A lot of the action on this front by our adversaries is taking place in these standards fora and China shows up in force to help push standards to create the kind of internet governance that they would like to see where states have much more power. They are not interested in the kind of open, multi-stakeholder, protection of human rights governance structure that we are interested in. And we have under-resourced and under-valued the importance of our participation in those standards bodies in advancing our national interests. So we've very strong on saying

we've got to step that up. And we've just got to be more strategic in our approach to how we collaborate with our allies and our partners and use these international bodies to advance our interests.

Rogers: I would agree totally with Suzanne. I think clearly there's a strong international dimension to our efforts in cyber. We can't just do this with a domestic-only focus.

I also think there's opportunity here. You've got a global community that is hungering for U.S. leadership. You've got a global community that recognizes cyber is an issue of concern to the entire broader world. This isn't just some small subset of nations. That represents opportunity for us and the State Department needs to be a big part of that.

I always thought the challenges was we just need to make sure that we're synchronized as a government entity. That what we're saying in one department reflects the action that we're taking in others. We've got to be consistent. And also to second something Suzanne said, particularly at the State Department I always thought about think strategically, think strategically, think strategically. Not in the day to day nuts and bolts of defending. That's what you have in CISA, DHS, Cyber Command, others, NSA. That's what they do for a living. We've got such a unique role that we just focus on what differentiates you from the others. We've got to maximize value.

Moderator: Scott Campbell, I see your hand up. Go ahead.

DWG: This may be a naïve question but Suzanne has stressed the importance of risk management. Does that mean deterrence is really not available to us? We're not going to counter-strike? If Senator Durbin's right, that's an act of war supposedly. Which wouldn't be allowed without the Congress. What is the role of deterrence in all this?

Spaulding: We were clear in our report to try to define what we meant by deterrence because that was a key element of our strategic approach.

What we mean by deterrence is altering the adversary's decision-making and that means altering their cost/benefit analysis. So people think about deterrence simply on the cost side. You know, we're going to impose some consequence on them for trying this

action. What we said is there's a lot more to it than that. Part of the cost is raising the cost to them by defending your systems better so it's more expensive. That alters their cost/benefit analysis. But also focus on the benefit side. Reduce the benefit that they gain through this malicious cyber activity. That's where the resilience comes in.

If you can have such a resilient electric grid, for example, that they really can't hope to knock it out for an extended period of time and have a huge impact on our nation, then they're less likely to focus their effort and energy on trying to bring down the electric grid.

So deterrence runs that gamut.

Having said that, that we need to focus on all of those, it doesn't mean, again, the fact that I say we need to assume that they're going to overcome everything and be prepared to deal with the consequences, plan it for right now, doesn't mean that we don't also have a piece in which we look at how do we make sure we can impose some cost, some consequences, right? So that's what I talked about at the outset which is we have to have a pretty big tool set, toolbox of ways in which, because if you only have one tool, a big hammer, you may be more reluctant to use it, right? If you have more tools, if you have a smaller hammer. If you have a scalpel, if you have, then you can use the appropriate tool given your level of confidence, given the seriousness of what you're trying to respond to. You don't have to let everything go that isn't hammer-worthy and not respond at all or use a hammer when it's not appropriate. You have a toolbox that allows you to respond appropriately. And I know that folks might work with and other folks around the government are working on fleshing out that toolbox, but at least when I left it wasn't where it needed to be and I think Mike would agree on that.

Moderator: Mike, what do you think of the toolbox? And does Solar Winds call for a hammer?

Rogers: A couple of thoughts. First I want to talk about deterrence for just a minute. It's one areas where I would give the Solarium Commission particularly high marks. I think deterrence remains a valid concept in cyber. I think the idea of shaping behavior and imposing cost, those are good fundamental principles to build around in creating a deterrence strategy.

I always thought the challenge was at times we thought about deterrence way too narrowly. To me I thought deterrence is about a host of options, and just because somebody comes at us in cyber doesn't mean we've got to go back in cyber. We've got to play to our strengths and we have so many strengths going for us. We need to think more broadly.

Now Frank you wanted to pivot a little bit. I wanted to make sure I got the question. What did you want me to make sure that I focused on?

Moderator: Is it time for the big hammer?

Rogers: Again, my comment is the big hammer for what? Before I start throwing hammers around I'd like to spend some time defining, so what is acceptable, what is not acceptable? Remember, this reminds me a little bit, I go back to Syria. We kept talking about red lines and this is unacceptable and we will never -- and then we didn't do anything. So my attitude is before you start talking about throwing big hammers around, make sure you truly understand what your concepts are here and what truly is acceptable and not acceptable, and then create a strategy accordingly. But don't start out with oh, the answer is we're going to the big hammer straight out of the boat. I'm like that is not the first thing I would do.

Moderator: Hold your hammers and don't draw your red lines until you're ready.

Another question. Solar Winds is a private company selling IT management software to the U.S. government and other companies. Do they bear any responsibility? If so, to what extent? Is there anything the private sector should learn from this and do different?

Rogers: The bottom line to me is yes, they have a measure of responsibility. But look, there's no one party, there's no one group, there's not one organization that we can point at and say this is all your fault. That's not the way cyber works. If that's what you want I think you're doomed to be frustrated and unhappy.

The reality is the complexity, the hyperconnectivity, the way we've created this worldwide web. It's interesting and it's

hard. The Russians turned the very structure of the worldwide web against us. We created this entire infrastructure with the idea that remote access on a regular basis to enable us to upload new software that gives us better functionality, more options, increased security and better efficiency is an inherent aspect of this world we created. And you watched how the Russians said to themselves, you know, that's a great vector for us to get in because the system is built to assume in many ways that that's all valid. That it's a legitimate activity. Hey, I want to go to a site like Solar Winds and I want to download their software.

So there's no one single answer here but I think it does highlight one thing among many that I would highlight for the private sector, and this is true for government. Supply chain, supply chain, supply chain. We have got to think much more broadly about what does supply chain mean in the digital world of the 21st century and we haven't really done that historically.

But Suzanne might have a different view.

Spaulding: As you know, Mike, we've talked about supply chain security for a long, long time and we've had task forces and folks have worked hard on this. It's a really, really hard issue and we are not even close to solving it, if you will.

So I agree with your assessment. Even though folks have worked hard on it.

I don't think we really know yet ultimately how Solar Winds' software update came to be corrupted. We are learning more about the technical aspects. What were the things that they did and what was it they inserted and how did they insert them, et cetera. But I'm fascinated by the SEC filing that Solar Winds, the documents that they filed with the SEC within days of the publication of the hack in which they made clear reference to a manual, I think was the word they used, pack of their supply chain. And I still don't think we have a clear explanation of what that means. So was this an insider threat? Did they mean someone who had physical access to perhaps the servers that were being used by the developers in the creation of the software and the update? We don't know.

So in terms of assessing the degree of their liability, I think we don't have the facts to sort of come up with that. I don't think we want to assume a strict liability. Clearly, their

product was corrupted and was the vector. I do think they should bear some responsibility but I think we can't know the degree to which they -- there's been a lot of talk that they may not have been as careful about cybersecurity as they should have been. And it may be that they weren't careful about personal, personnel security, physical security as they should have been, so we'll have to wait and see on that.

Ultimately, I think we to -- it's really hard, again, but I think we have to operate on a zero trust assumption. You've got to configure your system accordingly. This is why the basic things that we've been talking about forever, about making sure the only people who have widespread administrative privileges are people who absolutely need those. That your system is segmented. That if somebody gets in someplace they're not able to have free reign inside your system. All those basic things. We need to start assuming, as I said at the outset, those that have been victimized by this hack need to assume until they've scrapped this and started from scratch that the adversary's still in their system. And everybody needs to not get too complacent about the security of their third party vendors.

Rogers: In fairness to Solar Winds, I suspect as we gain more knowledge we're going to find out the Russians used multiple vectors, they used multiple approaches here and it wasn't just Solar Winds, even though that has gotten the most attention.

Moderator: We have some incredibly knowledgeable people and some journalists who dig deep into this in this group. I wonder if I might turn to one or two of you and draw you into the conversation if you're still there. Mark [Inaudible] you've spent a lot of time digging deep. We'd love to have you jump in here and put something on the table if you're still with us. Or Paul Shinkman over at U.S. News. For those of you who are covering this all the time and living with it, where this is going, what this new administration is going to do is going to be your big story and a lot of big stories going forward. So Mark, if you're there do you want to give it a shot?

DWG: Sure. Thank you.

I'd just be curious, a few weeks ago the dual hat was back in the news and that's clearly an issue that's going to be facing the Biden administration, so I'm curious to hear your thoughts on maybe the merits of keeping or severing the dual hat relationship

between U.S. Cyber Command and the NSA.

Rogers: An issue I wish I could tell you I never had to deal with, but I did deal with two different Presidents on this.

What I always said was number one, remember that the party should be ensuring both organizations, whatever configuration you want to go with, you need to ensure that both organizations can execute their mission. So don't make a choice that increases the risk of mission failure or mission degradation to either of them.

So when this came up before, when I was in the job, I never once said we have a set of criteria that we should use to make this decision. In fact if you look at the 2017 NDAA, we ghost-wrote what the criteria should be. That applied eight specific things. You should not look at separating these in terms of having one individual be the Director/Commander until you are confident we have addressed these eight specific areas.

As an incoming team what I would suggest to them is you need to look at this independently. You need to assess what's the readiness and the capability of both organizations. What are the options here. And is each organization ready to shift to a different structure without compromising its ability to execute its mission.

If the answer is yes, I have also been on record as saying in the long run I thought it was the right thing to do. There's only three of us who have done this, and Keith feels very strongly you should keep them aligned. Paul has publicly said just don't do it before they're ready. I have said don't do it before they're ready. But I think in the long run separation in terms of one individual doing both -- remember, they are always going to be aligned with each other. Cyber Command, for example, has no independent infrastructure. All of its infrastructure is resident within NSA facilities. Unless you want to go out and spend hundreds of millions if not billions to create unique infrastructure for Cyber Command, and I would argue we've got higher priorities than that right now.

In the long run, though, I always thought asking one person to be one of the 11 senior most operation commanders in DoD and running the largest intelligence organization in the world outside of Moscow, Beijing, Pyongyang or Tehran, there's a reason why I was at work at zero-five every day and I didn't go home until, if

there was nothing going on I didn't get out of there until 8 or 9 o'clock at night. And I was working seven days a week for four years. I just thought, you can do it, but is this really optimum? Now maybe it's just Rogers was incredibly inefficient and not very professional. That could be.

The other thing for me I always thought was a little bit of competition can bring out the best in both organizations and I thought both organizations really had some amazing capability. And that wasn't true three years ago. If you had asked me this question three years ago, I would have said uh, I'm not sure. But bottom line, identify the conditions, do a review and then make a decision. Don't go in with a preset yeah, the right answer is to this or the right answer is to do that. You really need to roll up your sleeves and take a look at it today.

Moderator: Sean Lyngaas from CyberScoop. I wonder if you'd like to bring your reporting and your perspective and a question to the table.

DWG: Sure, thanks for the opportunity and thanks for the discussion. It's a very good one.

Admiral Rogers and Suzanne Spaulding, would you mind just sort of elaborating on -- I know we've touched on it but what aspect of this espionage campaign may have breached norms in cyber activity? I've talked to a lot of people who think this is espionage per usual and the idea of setting ground rules around this is fallacy because the U.S. and its allies also do espionage obviously.

On the other hand, folks like Microsoft, Brad Smith at Microsoft argues that because of the sprawling nature of the operation that sort of undermine trust and fundamental pieces of the software supply chain, that that is a red line that shouldn't be crossed.

If you were raising this topic in a new administration what would you focus on in terms of norms?.

Spaulding: I'm troubled by the notion that first of all, if it's just classic espionage, spy versus spy, we do nothing about it. That's never the way we've handled it in the physical world when we find espionage going on, when someone's trying to suborn an agent in the State Department or what have you, right? There are always consequences, so I start with that.

You don't get up on your moral high horse and go around the world saying shocked to find gambling going on here but it doesn't mean you don't do anything.

I think the idea that this is different, that this isn't, as Frank said, mere espionage is right on two fronts.

With the OPM hack, for example, the point that we made and I know Clapper was quoted as saying something to the effect of good on ya, we do the same and good for you that you succeeded. But many of us felt that the OPM breach was beyond that traditional spy versus spy in part because of its scope and scale and the fact that the information that they took included very personal and detailed information of family and others who had no relationship with the government. Right? So there were sort of innocent victims. The scale of this took it into a different category.

And I think similarly here with this massive hack by Solar Winds, they did not stop with government agency. Right? They went and potentially now had access to 18,000 victims, many of whom in fact even of those that we apparently have identified as having downloaded the update and triggered the malware are mostly private sector entities.

So again, I think we worked on norms that said you should not disrupt critical infrastructure upon which citizens depend, for example, and we were prepared to live by that norm and we thought it was something that others should live by as well.

So I think we still have to learn more about the scale and scope of this hack but I think even given what we know already, that we are within, that it is appropriate for us to suggest that this goes beyond traditional spy versus spy.

Rogers: I would agree with Suzanne. This isn't just a traditional espionage because of the private sector dimension to it. It wasn't just valid national security targets, so to speak. And again, because we don't yet have a full understanding of this. I'm leery about drawing conclusions very early in this process because we don't truly understand the nature of the activity, the full breadth of the targets, what were they doing, what did they do? I'd want to understand that before I start making pronunciations about this is unacceptable, that's unacceptable.

It does highlight, though. You know, you always wonder, and I don't know if it crossed Suzanne's mind but it certainly crossed my mind when we sit and debate some of these things, what is it, what are the criteria we're going to use to decide something has crossed the threshold?

I can remember, I thought for sure Sony in November of 2014, a foreign government uses malicious software to physically destroy U.S. infrastructure in the form of a company, Sony, as well as steal their intellectual property -- emails, their films -- as well as release the information in an attempt to embarrass Sony. And yet we ultimately decided well, this is about law enforcement. It's a legal issue. It's a breaking and entering theft kind of thing. And I can remember saying in the sit room, would we be having the same conversation if this destruction occurred because somebody out a Tomahawk missile into a building? What is it that makes the destruction by software inherently different than destruction by physical means? Because if we can't articulate to the broader world around us this idea of a framework for what is acceptable and not acceptable -- we generally use the buzzword norms in many ways to describe it -- we can't get to long-term stability in cyber if we can't come to some kind of consensus.

I also think that desire to generate consensus again offers us great opportunity in an international [inaudible]. I would not be addressing this specific hack purely from a U.S. perspective. We're also going to find there's a dimension of foreign targets, non-U.S. targets in all this.

Moderator: Any point in the Biden administration taking on negotiations with the Russians and trying to set rules of the road here?

Rogers: I would not start by starting with let me negotiate with the Russians. Rather I would say between ourselves, our friends and our allies and the broader global community, what do we collectively think should be a basis for acceptable or not acceptable? Then I'd be talking to the authoritarian states about hey look, we've got a bit of a global consensus here. We've tried to do this for years and Suzanne and I were both part of these discussions and efforts to do this in the past. But there's no easy answer. I'm just a little leery about let's not go high and right, this is an act of war, let's pull the hammers

out and start -- I don't want to speak for anybody else, I'll only speak for me. I'm going, let's think a little bit here before we --

Moderator: Yes or no, Suzanne, you agree with that? Don't start with the Russians? Don't waste your time there?

Spaulding: I don't think Mike was saying don't waste your time there, ultimately.

Rogers: I was not.

Spaulding: You don't come in on day one and say okay, let's sit down and talk to the Russians, let's sit down and talk --

Moderator: It's about leveraging, about maximizing your time.

Spaulding: It's about having a strategy where you thought several steps ahead. What is the outcome that you're seeking? Are there things that need to be done first by Russia, by China, others that make for a constructive negotiations to proceed? Right? Are there people, shorthand is preconditions, but are there things, assurances, what have you that need to precede those kind of direct negotiations so that you can believe that you're going to have constructive progress there?

But Mike is absolutely right. We should talk to our allies, our partners, and say what are our strategic objectives here.

Moderator: We have about four minutes left. Sean, did you get what you needed?

DWG: Yes I did. If I could throw one more question in there.

Given the relatively high standards of the press and the public have had for attribution in recent years in terms of U.S. government coming out publicly and saying who is behind a sophisticated operation, I'm wondering how you expect the Biden administration to treat that because this particular espionage campaign caught a lot of people off guard and a detailed attribution statement might take a while. And also might require revealing sensitive sources or methods given that it was a surprise, and I would imagine but don't know that intelligence agencies are going about their business right now trying to figure out what's going on by conducting their own operations.

Rogers: Again, it's one area where I would give the Trump team some good marks. We saw public attributions by the government more aggressively in the last four years than the previous four years probably. Again, I was part of both teams.

I think that public attribution can be a powerful tool. I just would urge you need to make this on case by case basis. I would not default to a simplistic everything is automatically public attribution nor nothing is public attribution.

Spaulding: And Sean, you make a good point. Does a public attribution by the government need to be followed with the degree of convincing evidence that you'd have to present in a court if you were making a criminal case. I think it should not have to be. I think we should set public expectations accordingly.

The other aspect of attribution is that it is often the private sector folks, often private researchers, academic institutions, whatever, that are fastest on the attribution and able to come out with attribution. Some of them have gotten gun shy because they've been retaliated against. And one of the things I think we could think about that I've heard suggestions and I think it's fairly creative is to set up a third party sort of consortia that might make those kinds of attributions on behalf of its members so that no one member is singled out for criticism, challenge or retaliation. But I do think attribution is obviously a critical part of accountability and deterrence.

Rogers: Real quickly to that point, I always thought attribution was most effective when it combined the insights of government, the private sector and the broader international community. When we brought those three components together it was incredibly powerful.

Moderator: Sarah Friedman, if you're there and you want to have a last question from the crowd it's all yours.

DWG: Thank you. When it comes to the creation of a National Cyber Director which is supported by the Biden administration, one of the key challenges they will becoming in with is the Solar Winds hack. Industry has talked a lot about how this could be a potential point of coordination with government officials. What do you think some of the priorities of the Cyber Director Office going forward is and how will Solar Winds be part of that?

Spaulding: There are pieces of the Solar Winds hack and our understanding of it spread out across government in the various departments and agencies that are in there doing battle right now that have been impacted, and obviously these many private sector victims and the cybersecurity firms that are helping them and companies like Microsoft that also were part of the technology deployed here. So it is a perfect opportunity to start off on day one operationalizing the kind of collaboration that we are looking to this National Cybersecurity Director to bring. Bringing the private sector folks to the table as well as across the interagency and our allies overseas who may have insights for us. And working hard to share more information than we are normally comfortable sharing.

Mike was always pretty good and pretty forward-leaning on telling his folks we need, this information isn't going to be any good if we can't get it to the people who need it and can use it. But there is still an awful lot of secrecy and we are not going to give enough clearances to folks to solve this problem. We've got to get more comfortable sharing information and our Solarium report talks about some of this starting with systemically important critical infrastructure where we would share more sensitive information.

But this is, as you point out, this is a perfect opportunity to not just do information sharing but to collaborate on an operational basis. Who has the capability to do it and how do we empower them to do it?

Rogers: I agree with everything Suzanne had to say. Bottom line, if I was in my old job what I would be telling the team is every crisis is opportunity. Crisis and opportunity enable us to drive change in bureaucracies that are often resistant to change. It's amazing what bureaucracies are willing to do when their reputations are on the line and we're all dealing with embarrassment and we're all trying to recover from a situation that should not have occurred.

Let's take advantage of this, you guys. Let's not hang our head and say oh, my God, we're worthless because we failed to let this happen.

Moderator: Every crisis is an opportunity. There's a lot of opportunities right now.

Rogers: There is.

Moderator: Before I let you go I want to play a little game with you. I'm going to play the elevator game with you.

Suzanne, you're on an elevator, you get on on the 8th floor. On the 7th floor the doors open and in walks Joe Biden. The two of you get to go down to the lobby together. What do you tell him he needs to do in the time you've got in this very challenging cyber area?

Spaulding: I would say you need to fully empower your National Cyber Director to bring everybody to the table to make sure we understand who has what capabilities, what resources and what authorities and that we are fully maximizing and aligning those resources and missions and empowering people to do what they are in the best position to do. One of the first places that he has to be thinking about this is COVID-19 and the potential for cyber disruption of that vitally important effort.

Rogers: For me, you've got a great set of challenges, but you've also got opportunities. Remember, this is going to take sustained commitment every day you are in this job. I wish I could tell you, sir, that you are going to fix this in a month, in a year, in a single term, in a single administration. That is unlikely. This is about focus, this is about prioritization, this is about leadership and emphasis. This is about harnessing the power of the government to work with others to come up with collaborative solutions, many of which are outlined in the Solarium Report. Look, we can do some great things if we're wiling to work as a team.

I guess the only other comment I would make is, and I saw this not with the incoming team, but I was always struck at times having worked with multiple administrations, I was always frustrated, stop taking the attitude that everything my predecessor did was wrong. Come into this with hey look, I've got the responsibility. It's my responsibility now. What can I learn, how can I build on rather than hey, I'm just going to blow everything up. I don't think they're going to do that, but I would sure hope, because I've seen that occur before where I just oh, my God, we're walking away from good work. That doesn't mean it's perfect, but why don't we view it as something to build on not something to destroy.

Moderator: I'd like to have a conversation about where you saw that before and what shape it took but that will have to be a sequel to this conversation.

I would like to thank you both for tour time and your insight today. IT's been great and fascinating, and the journalists who joined us. And Admiral, I'd like to thank you for your 0500 to what time did you say you went home? 8, 9, 10 o'clock at night? I'll bet it was more than that, and Suzanne, same for you. We thank people for their service and sometimes it's sort of a punctuation at the end of a conversation but I think we really especially with what we have seen in recent days need to take a moment to thank people for the work they put in for this country under whatever circumstance they do it when they're doing it for the right reason, and you both have done that. So thank you for that as well.

Rogers: It was an honor to get to work with people like Suzanne. There are some great people who are working hard, as there are in the private sector.

Moderator: There really are. I wish the public got more of a sense of that as well.

I also want to thank David Ensor who does an unbelievable job as the Director of our Project for Media and National Security and David, I'll hand it back over to you.

DWG: Thanks to everyone for what has been to me a fascinating conversation.

# # # #