Anja: And the US government and businesses have become essentially a permanent feature of the landscape. They are sometimes state sponsored, sometimes countries such as Russia and China turning a blind eye to groups operating inside their territory. And we've seen all of the following in just the past couple of months, increased ransomware attacks on hospitals and health care facilities, hacks on major supply chains and critical infrastructure like SolarWinds, Colonial Pipeline and others, a major executive order from President Biden in May pushing for stricter cyber security controls.

And of course, the woman behind many of these policies and really trying to keep our country safe is Anne Neuberger, who is with us today. She is the deputy national security advisor for cyber and emerging technologies. Previously she was the National Security Agencies, the NSA's director for cyber security. She also led NSA's election security effort and has had many, many other distinguished roles in the US government. We're very proud to have her with us today.

And of course, interviewing her today could be none other than our own David Sanger, member of the Aspen Strategy Group, old friend of many of ours, and really one of the foremost journalists at the New York Times writing about cyber issues. I think he's won too many Pulitzer Prizes to mention. And he also wrote a book recently called The Perfect Weapon that examines the emergence of international cyber conflict. And I have to brag about David a little bit. The Perfect Weapon was just released as an HBO documentary and I think is now Emmy nominated. So Anne, David, thank you very much. Welcome to the platform and I'll hand it over to you.

David Sanger: Well, thank you very much Anja and thank you Anne for joining us. Since Anne came in as the deputy national security advisor for cyber and emerging technologies, I think we've all seen a huge level of activity, new policy. She's been out speaking about this including here today, so we're delighted to have her join us. She's been talking a lot about the administration's policy. And I think everybody agrees that it is much more activist and that she's now of course joined by Chris Inglis, the national cyber director and Jen Easterly who's just been confirmed running CISA over at the Department of Homeland Security. So there's quite a team together. Anne, thanks for joining us today.

Anne Neuberger: David, thank you so much for having me here. It's great to be here and great to have a conversation with you, you've invested so much time and just knowledge in this space as well.

David Sanger: Well, thanks. Anne, I wanted to just start with the three areas that you've been talking about the most in dealing with this strategy. You've talked about all of us getting healthy. We just saw the NSA last week suggest we all get off public wifi, good idea probably five or 10 years ago and even better today. But you've had many other steps, including the executive orders. You've talked about working with allies and you've talked about using all capabilities, which I assume is sort of a code word for how the US could use sanctions, it could use indictments, it could use offensive operations. So will you walk us through those three before we drill down a little bit on ransomware and other challenges you're facing?

Anne Neuberger: So we thank you so much, David, and Anja a moment ago, thank you so much for the introduction as well. So cyberspace will really be a key consequential area of geopolitical competition in the 21st century. And some of the leading threats to the American way of life are cyber enabled, espionage influenced to attack. So the administration in cyber strategy covers the three areas David noted, first to fortify ourselves at home.

First modernize our defenses to essentially meet the threat. And when we talk about modernizing our defenses, there're really three areas we're focused on. First, using the federal government as an example, and you've seen the administration rolled out an aggressive, but achievable, we believe, executive order with very clear timelines to ensure the federal government becomes a leading example of cybersecurity resilience. Second, a key focus on critical infrastructure and just a number of innovative ways to partner with the private sector recognizing that 85% of critical infrastructure is held in private sector hands.

The efforts underpinning that including the president's industrial control systems initiative, which has allowed for cybersecurity technologies to be rolled out to 150 utilities serving 90 million Americans as well as creative ways to bring the private sector in to respond to a major cyber incident like Microsoft Exchange. Including finally, among modernizing defenses, the third leg of that really innovating on using the power of federal government procurement to get at the root causes of our cybersecurity issues.

The absence of visibility into the risks in a given software product that we buy as companies, as agencies, as individuals, the absence of transparency into what is actually in a product. And finally the absence of labeling so that even if a mom wants to buy a secure baby monitor, she actually has a sense of what is a more secure baby monitor. So across all of those areas and I'm happy to go into more depth on any of them, the president's executive order on a number of key initiatives like I described, have really made forward progress on modernizing the nation's cyber defenses to meet the threat.

The second key line of work is really leading internationally. Our allies and partners are a tremendous source of strength and unique American advantage and our collective approach to cyber threat information sharing and mitigation as well as holding countries accountable for meeting cyber norms is a key line of work. So we've really expanded diplomatic engagement in that way.

You saw the announcements, for example, at the G7 and the EU commitments around ransomware. You saw the NATO update to a cyber policy for the first time in seven years and you saw an unprecedented number of countries join us in attributing the Microsoft Exchange hack and really calling out the irresponsible behavior that underpin that. So that's been a big piece of that as well as our efforts on emerging technologies and on standards related to that in terms of really leading internationally and recognizing that we're more effective bringing countries, allies, and partners, learning from them and working with them closely. And then finally, posturing to compete to ensure that we can fully be able to compete on the global stage with all elements of national [inaudible 00:07:23].

David Sanger: Well, thanks, Anne. Let's go into a couple of examples of how you've responded to some of these. Of course, before you came into office, you were dealing first with the Russian attack now attributed to the SVR which looked to be the most... this was of course the SolarWinds attack look to be quite different because it got into the supply chain, the supply chain of software. In that case, the Russians actually spent, looks like more than a year, figuring out how to get into SolarWinds' code knowing that it would flow its way into government institutions, think you've said about 10 federal agencies.

And of course, we know that they hit more than a hundred of the major corporations out of 18,000. And then of course, shortly after that, you had to go deal with Hafnium, the attack that China led as you attributed recently on Microsoft Exchange systems. Both of these seem to be of a different nature and required you to go bring industry right into the situation room, take people who were cleared and deal with them. So talk to us a little bit about how this was different from the way these have been handled in your many years working on corporate engagement when you were still at the NSA.

Anne Neuberger: Absolutely. Thank you so much for the question, David. So as we looked at SolarWinds, what we were struck by was the degree as you know of sophistication and investment and building out a capability again of the supply chain. And that one is, as I noted earlier, very difficult for consumers of that technology to detect. So our approach in addressing it really covered the three aspects of the administration strategy, first modernize our defenses.

You saw in the executive order a key component which we said the US government will only buy technology which is built in accordance with software security standards. We tasked NIST to develop those software security standards on a 60 day timeframe. And right at first, they brought in the private sector in defining new standards over almost a thousand participants and then right on time on the 60 day mark issue those software security standards and how software is built.

And clearly that doesn't just benefit the federal government. We, companies, agencies, companies small and large all use the same software. So by the federal government defining the standards and saying, "When we use the power of our procurement to move the market there, we're benefiting small, large businesses, individuals alike." So that was the first part of our response to SolarWinds. You saw the second part, which was bringing countries along with us when we attributed that to the SVR and filing the statements around seen and unseen consequences as well.

When we look at Hafnium, what was troubling about Hafnium or China's MSS compromising tens of thousands of Microsoft Exchange servers around the world is that it's a broadly used commercial tool and almost traditional espionage and identification of a vulnerability. What was unusual was the broad, we might call it, irresponsible compromise of tens of thousands of computers around the world.

I would contrast that to where when the US government specifically the National Security Agency found a broad Microsoft Exchange vulnerability shortly thereafter that was quietly shared with Microsoft to allow them to patch the vulnerability and release that patch because of the focus on recognizing defense in such broadly used products has to be a priority. But then noting the attribution, an even larger group of countries joined us to collectively call out the behavior as irresponsible and to note that that kind of broad compromises were really outside the norms of acceptable nation state behavior in cyberspace. So you saw that focus on those aspects of our strategy and leading internationally in both aspects of them, but somewhat different in the overall approach that we felt was needed to counter the particular threat.

David Sanger: Pardon me. Anne, let me ask you a little bit about the differing responses to the two countries. In the case of SolarWinds, you did sanctions publicly against Russia, you did not against China. What was the theory of that?

Anne Neuberger: As we've noted over the last number of years, SolarWinds was not the first case. Are you okay?

David Sanger: Pardon me.

Anne Neuberger: SolarWinds was not the first case of aggressive Russian cyber activity in the international space, there've been a series of activities in Ukraine, in Georgia, activity in Europe as well. And there's a broader consensus around the need to call out that behavior and improves costs, running costs is a significant one. In the case of China, there's still that building of consensus around malicious cyber activity around the need to call it out together, work collectively on defense and work collectively on consequences as well.

You did see the Department of Justice indictments related to that, but you saw us take the more step-by-step approach of building that consensus, bringing countries along, establishing that norm in the case of the Microsoft Exchange hack, which doesn't preclude follow on activities, but emphasizes the Biden administration's approach to not go at it alone, but instead to use a sequential, thoughtful approach to bring partners along, establish those norms of excessive behavior in cyberspace and then take it from there.

David Sanger: I have to ask you about one of the critiques of the way you've gone about this. Our friend and colleague Jack Goldsmith at Harvard Law School who you and I have dealt with a lot over the years, wrote a piece back in July called Empty Threats and Warnings on Cyber. You may have seen this in Lawfare. And basically it walked people through the various moments that President Biden has talked about taking direct action, raising the cost dramatically for bad cyber actors, mostly Russia and China.

He started this during the transition in December 2020 when he said about SolarWinds, "We can't let this go answered. Cyber tax must be treated as a serious threat, we'll take meaningful steps." And I think you've described some of those. And then he also said, "We would respond in kind." That may have been the unseen part of what you were discussing in seen and unseen. And then again, in June, when we were in Geneva, I asked him at a press conference about if these kinds of attacks on critical infrastructure continued how he would respond and he said there would be a cyber response onto these.

We haven't seen those in public, maybe they've happened in private. And I know you can't say if they have, but Jack raised the interesting question, said, "Any such message should have been sent only once. The reason to send it would be to establish red lines that if crossed would be met by a response more painful than the gains of the action. But this is clearly not what's been happening." And that time and time again, he wrote, we kept saying, "If Russia uses these weapons, does something bad and that's met with another operation and just more warnings and threats." So he's basically saying we're in a cycle here. I suspect you probably don't agree with them, but I'm wondering if you could address it.

Anne Neuberger: Absolutely. So I'll take a step back there for a moment. And I think what we've seen is President Biden engaging directly with President Putin outlining concerns, outlining very clear outlines of what is unacceptable behavior, describing that, establishing an experts group to continue to build out the next level of work on that and really define-

David Sanger: An experts group with the Russians?

Anne Neuberger: Yes, [crosstalk 00:15:53].

David Sanger: And that's been meeting and are you learning much from that?

Anne Neuberger: Yeah, I'll get to that in a moment. Defining that, defining clearly our expectations and frankly, our bilateral expectations to say much as we would expect of any country to address aggressive cyber behavior from within its borders, particularly if it's having a disruptive impact on critical infrastructure in another country, we expect the Russians to address this behavior and we commit to addressing any similar behavior the Russians identify of ransomware activity coming from within the US against Russia. So that was an important step.

You haven't previously seen a president engaging both in private and in public to define our expectations, define that norm. It's a previously established norm under the UN governmental group of experts and really make clear our expectations in that way. The second of that aspect is the deterrent aspect of the very public investments of money and effort and time US government is making to modernize our defenses, to launch innovative, critical infrastructure resilience efforts.

We've made a massive push to really say we must address our poor level of national cyber resilience in no small part underpinned by the fact that critical infrastructure is owned by the private sector. And we must encourage, incentivize and move the private sector to make the investments needed to ensure that we as a country can guarantee those critical services. The final aspect to your point is potentially other ways to impose costs. That needs to be a final aspect.

We've conveyed that that is an option, but we want to work through what we can to ensure that can we the most effective way to address ransomware and other disruptive cyber activity coming from within a country's borders is within that country's leadership, shaping their expectations and shaping their calculations. And I think you've seen the president doing that in a very thoughtful way across his personal engagements, the engagements he has built across our country's inter-agencies and also in that approach, both to bolster national resilience, engaging allies and partners and making clear that other options would be considerably small.

David Sanger: And you've often made the point, and I think did when you were still back at NSA where of course you ran operations for a while, and of course you were doing the public private sector engagements, that while offensive operations can be emotionally satisfying, you've struck back in some way, they're frequently not very lasting or very useful. And I was wondering if you could talk people through that a little bit because something that you see a lot in ordinary commentary on this is why don't we do back to them exactly what they do to us? Say up and apart from the values issues that that raises for the US, so what does your experience tell you about the limitations on the utility of just striking back?

Anne Neuberger: It's an interesting question, David. I think it was former secretary, Bob Gates, who talked about the unpopular question of what comes next. And that's really foremost in our mind as we often think about it. We know we overall as a country have all kinds of different options that we build to ensure we can hold adversaries accountable, but we always have to think about the long game and say, "What is our ultimate goal?"

And ultimately our ultimate goal is to keep the nation safe in cyberspace. As I noted, it's a very consequential area, particularly currently. And with that long goal, we say first deterrence by denial. Let's get ourselves strong at home. Second, let's build those international norms about what is expected and what is responsible behavior in cyberspace and then let's ensure that we have the capabilities necessary to defend ourselves.

But given the level of national resilience, and this is a core part of now that was underpinning our ransomware strategy, given the fact that we do have gaps in security across our critical infrastructure, we knew that addressing that first and foremost with priority was as important and thinking carefully about what comes next with any other options we consider are needed. But clearly in executing cyber operations, one must always consider the interoperability of networks. Having a discrete impact, having confidence in that discreet impact is often challenging given how much networks are interconnected within countries and globally as well.

David Sanger: So part of what you're saying to us is because we haven't built up our resilience yet, and you've made the point we are years behind where we should be. We haven't sort of gotten our act together. And that's a limitation on our ability to use offensive. So this is as Bob Gates always says the three words least asked in Washington are, "And then what?" So in other words, you couldn't really control the escalation if you just routinely use an offensive weapon back. Am I summarizing that right?

Anne Neuberger: I think rather than limitation, I would say it's a factor in thoughtful consideration of options and strategy.

David Sanger: Let's move on to ransomware, the main subject of the president's conversation with Putin. So as they headed into Geneva, you had just been through Colonial Pipeline. I think an incident that really grabbed people's attention because it managed to really declare to people that this is a major issue that can affect not only your computers, but your gas lines and so forth. The second attack that you then saw was against a major meatpacking industry. And then of course, we had the meeting in Geneva, the president said this has got to stop. He gave President Putin the 16 areas DHS has noted as critical infrastructure.

And then of course we saw another attack. And just in the past few days, we've seen recorded future come out with a long interview with what seems to be a weak constituted version of DarkSide, a group that I think called themselves DarkMatter or something like that said that they have learned the lessons. They weren't going to attack critical infrastructure, but they were going to be back and bigger than ever. So is this group... I'm sorry, it's Black Matter. Is this group Black Matter just the revival of DarkSide? And does this suggest that the Russians haven't gotten the message yet on ransomware?

Anne Neuberger: It was a remarkable interview in the insights of Gate and into the state of mind and the way the particular group approaches ransomware activity. I would say it was remarkable for some of the things that were said regarding avoiding critical infrastructure targets, regarding a working group that had been established. So while I think we've observed a number of overall comments by Russian government officials following the summit, we saw the director of the FSB note on interested in partnership to address cyber-criminals, you've seen other related comments.

So I think as we looked at that interview, we took it as evidence or perhaps as a sign that the message regarding the disruptive ransomware activity against critical infrastructure is unacceptable and we will address it. We felt that that message was reflected in some of that. Now, of course as my boss Jake Sullivan said and I think as the president has made clear, the proof will be in the pudding.

We're looking to see the changes addressing disruptive cyber activity over time. But we think we're seeing a commitment and we will look to see the actions that follow up on that commitment. And as we said, we view this in a bi-directional way as we're prepared to act as well if issues are highlighted to us about cyber activities.

David Sanger: So what you're saying to us is the fact that the extensible Black Matter representative speaking to recorded future, assuming these people were who they said they were, the fact that they said we will-

Anne Neuberger: [crosstalk 00:24:32].

David Sanger: Yeah, it's a big caveat. Assuming that it's accurate, the fact that they said, "We will avoid critical infrastructure," tells you your message is getting across. On the other hand, if you're a company in the United States or elsewhere that doesn't deal in critical infrastructure, it was also saying you're still a major target.

Anne Neuberger: When we talked about our ransomware strategies you noted. We said our first goal is disrupting the ecosystem that feeds ransomware. At the end of the day, it's the old joke about what's driving ransomware. To a certain extent, it's where the money is, right? We're seeing the growth in ransom payments, et cetera. So I think when you look at our ransomware strategy, there's four parts to it. Piece number one is identifying disrupt that ecosystem, identify who the actors are, identify the movements of virtual currencies that enable it.

The second part of that is work with our international partners to put in place both increased regulatory focus on virtual currencies in the United States. The United States is a leader in this space. Treasury has been made active working space in the last number of years by the Financial Action Task Force, but double down on your customer rules and the regulatory rules that enable and ensure that elicit use of virtual currencies is addressed with more focus and rigor.

And you saw the president's pointed comments in the G7, building a coalition to address that, and we're taking some key steps on that. The third piece is the resilience piece. You saw the letter we issued calling on companies to do the steps they need to do, frankly, to do the steps the federal government has invested real money and effort in the five key cyber security areas that really reduce the risk. And then finally, as I noted, working with allies and partners to hold countries accountable who harbor ransomware activity.

So I think to your point, David, just taking a step back, we don't think any one line of that strategy is adequate. There's a reason there is four core lines of effort there because we think that all of them working together will both address the countries who harbor ransomware actors, show them that that's unacceptable, address the virtual currency enablers of it and build that international coalition while also calling on companies to say, "Lock your doors, right? Invest in your alarm systems." That's really a necessary area that's part of our national strategy as well.

David Sanger: Well, in the few minutes we have left before we go to some questions from the audience and I can see here, there are a lot already really lined up for you, no surprise. And wanted to ask you about a few of those specifics. So you've been reluctant so far to endorse the idea of banning ransom payments and ransomware cases, how come?

Anne Neuberger: It's a really good question. And I will say that initially thought that was a good approach, right? We know that ransom is... ransom payments are driving this ecosystem. And we said maybe banning that is the right answer. And then we brought in a lot of input, input from the private sector, input from a ransomware task force that really incorporated a number of former government officials, private sector leaders very effectively and had done a very thoughtful review over multi months.

We really took in a lot of that input and we heard loud and clear from many, but the state of resilience is inadequate. And as such, if we banned ransom payments, we would essentially drive even more of that activity underground and have both less insight into it that will enable us to disrupt it, but also not really address the root causes. So we said, let's take a step back, that's not an approach we can do at this moment in time. And instead, let's drive that four part approach to really both address the ecosystem, encourage and incentivize resilience.

Because our goal is just fundamentally decreasing the ransomware that's just affecting US companies large and small, and really state and local governments around the country, and frankly, our allies and partners around the world. There's almost no topic that when I talk with my international counterparts gets them ready to jump in on our coalition efforts or really interested in sharing information, learning from us, teaching us on ransomware because it's had such a disruptive impact on so many governments' abilities to provide critical services and on so many companies around the world.

David Sanger: But you've seen some cases with the payment of ransomware. It may not have been necessary. The JBS case, the meat packing... the meat distributor case, they paid $11 million and it's not clear that their operational side had even been attacked. In the case of Colonial Pipeline, they paid the ransom before there really had been many consultations with the US government. Did you find that disturbing?

Anne Neuberger: I won't speak to individual cases, but what I will say is we really press companies to say, "Make the investments in cyber security. It gives you a better return on investment." Put yourself in the position to know that you can defend your networks. Approach it in a way that really is focused on risk. One of the most formative roles for me was serving as NSA's first chief risk officer following media leaks.

And the focus on how risk is thought through what are your most key assets? Is it your reputation? Is it your intellectual property? It's your continuity of business and your operational networks. And we really encourage chief executive officers, don't make this a cyber thing. Bring in your executive team, ask yourself those questions and then invest in that resilience, it's the best investment you can make. We really believe that... we discourage ransom payments and believe they're fueling this ecosystem and are not the right approach.

David Sanger: Last question for you has to do with going to the other part of this, which is cryptocurrency. Yesterday we heard Gary, councilor of the FCC talk about his own thoughts about why we had to enforce cryptocurrency or look at cryptocurrency actions much more carefully and make them more visible. Of course, the IRS is interested in it because they fear that they're losing tax dollars. You're interested in it for a different reason though. You want to be able to trace these so the cryptocurrency basically does not become a way to pay these ransoms. Tell us a little bit about how that would operate.

Anne Neuberger: Absolutely. And Gary has been a very both innovative and thoughtful voice in a number of inter-agency discussions on this topic. So fundamentally, if we want to disrupt ransomware and money laundering networks, we need to be able to rapidly trace and interdict them around the world. And there's a lot of lessons learned from physical, know your customer and anti money laundering global efforts that we're working to apply here. There's things that are very different in virtual currencies.

And it's been really interesting to do deep dives, both with the private sector, deep dives with the intelligence community to understand that ecosystem, the exchanges, the mixers, the things that are anonymity enhancing and the perspectives of many that a big part of cryptocurrency transactions that occur. The kind of anonymous transactions that occur are often criminal transactions. But our driving goal is the rapid tracing and interdiction, and really the strengthening of domestic and international virtual currency regulatory environments to enable that.

We do believe value of virtual currency innovation. So one big part of it is also building in those cyber protections and the design of new virtual currencies and addressing that in a way that we can both have the innovation and not have the broad illicit use that's driving criminal activity.

David Sanger: And that would require congressional action obviously.

Anne Neuberger: There are efforts that we're doing across the executive branch, a number of efforts we're looking at here in that way, for example, potentially ensuring that all ransomware payments were notified quickly so we get better visibility into that. So there's a number of areas we're looking at in that space as well.

David Sanger: Well, Anne, you and I could do this for hours on end and at various moments we have but I feel like I've had all the fun here and not have a chance to let our great audience ask you some questions. So I'm going to turn it back to Anja with thanks for the time you've spent here. And Anja, I think you've got, oh, just 20 or 30 questions lined up.

Anne Neuberger: It's always great talking with you, David. Thank you so much for the time and as was always learning from you during our conversations.

David Sanger: Well, thank you, Anne.

Anja: Thank you, Anne and thank you, David. And Anne, your comments were excellent and did spark about 20, 25 questions. So without further ado, let me turn to Jane Harmon.

Anne Neuberger: Thank you, Anja.

Jane Harman: Good morning everyone. Am I up? Wait.

Anja: You're not on camera Jane, but it's okay. There you go.

Jane Harman: Yes, I am.

Anne Neuberger: There you go.

Jane Harman: Greetings from Aspen. I wish we were all in person, I just arrived here last night. And congratulations Anja to you and Nick for this extraordinary conference where I have learned a lot. I thought I knew stuff, but the last panel on the promise and peril of cryptocurrency, the promise part was really interesting. So on this topic, as David knows, I am first going to say that he wrote his amazing book, The Perfect Weapon at the Wilson Center and that we, the Wilson Center, where I was president and CEO for the past 10 years teaches cyber to Capitol Hill staff.

And with David's help, I think we have made some difference on the Hill. I have a two-part question. And the first part is that I didn't hear any conversation about a cyber regime, which I know comes up from time to time, and my question is how realistic is it that we could have a worldwide cyber regime with China and Russia in it that would make a significant dent in the use of cyber as the perfect weapon, the use of cyber against critical infrastructure et cetera?

And the second part of my question is that now as we just heard from Anne, and I think you too, David, that we are much more capable of attributing and naming and shaming countries and rogue actors who do ransomware, have we created somewhat of a deterrent which might, David, get this David, make cyber less of a perfect weapon?

Anne Neuberger: So it sounds like you had a question for me and a question for David, which sounds like a very equitable division there. Thank you so much. So as we look at recent progress on norms under the governmental group of experts of the UN, interestingly enough, Russia fully participated in that in defining norms of acceptable state of [inaudible 00:35:26] one of which, for example, is addressing behavior coming from within countries borders, second, providing support to countries, computer emergency response teams when they request help.

So I think we've certainly seen a willingness to participate in these voluntary norms, what responsible state behavior in cyberspace is. And now the question will be, when behavior is then flagged, do countries act on that? And I think that is the key place where we're at. So we're certainly hopeful. We believe that we can have countries agree to a set of responsible norms. And we think that the work we've put in frankly to that attribution and to bring in allies and partners along is a foundational step to enabling that. And that's really one of the reasons we've invested such effort both in the two attributions about administration in this time. David I'll turn over the second question to you.

David Sanger: Well, this is an Anne's moment, not mine. I'll just be very brief and say that I think that this is clearly an area where treaties don't work and what worries people about the norms is that Russia and China and others are trying to formulate those norms to fit authoritarian models, and that's what's going to make this so difficult. We've had the UN experts group that Anne referred to now for six or seven years. And we've seen a significant uptick in activity, including the ransomware activity in that time so that tells you that the guardrails we put on so far aren't working. And that's why I suspect that while it's a good start, it's got to get reinforced with making the costs far higher.

Anja: Right. Thank you, David. Thanks Jane and Anne. We now turn to Josh Wofford who is one of our rising leaders, inaugural class of rising leaders here at Aspen Strategy Group.

Josh Wofford: Deputy secretary, thanks so much for giving me the opportunity to ask you a question. As an officer in the military, a lot of our software is becoming more and more outdated. And with that, some of the security challenges we have pose frustrations and the delays with security and the way we handle security as far as passwords and all causes people to look for workarounds instead of being able to use the system in a way that enables it to be as secure as it could be. I know we've been updating things using two factor authentication and others as well. What are your thoughts on being able to modernize that government software that we use in a way that's safe and secure and makes it so that it's more user-friendly so people don't feel like they're forced to use work arounds that could potentially cause security lapses in the future? Thank you.

Anne Neuberger: First, thank you for your service and thank you for the passion, underpinning the question. I often think on any journey of change, it's important to both look over our shoulder and see how far we've come and then look up at the hill and say, "Darn well, we've got to double down and move there even faster." And I think security across DoD on the military is a great example of that.

On the one hand, duty leads for federal government agencies in having created a set of governance whether you work for the army or the air force, there's one governance around those networks that drives how quickly patches particularly critical patches have to be made drives modernization, drives upgrades in that integrated way. One of the things we did in the executive order was try to recreate that governance model for federal civilian networks to do that same focus threshold, common threshold of security in recognition of the fact that one vulnerability can rapidly move across a network and building in that segmentation is important as well.

So your point is incredibly well taken. DoD has come very far, it has a ways to go. And frankly, to your point, cybersecurity technology drives innovation as well, and really thoughtfully thinking about ensuring that we have that innovation, but also knowing that we have a way to rapidly identify an intrusion and rapidly block that, and also quickly look around a network to identify other evidence of that is important. So I think good progress made, a lot more to be done. And I would particularly call out the efforts that are being put in place around cyber hygiene, rapid patching, multifactor, you noted are some of the really key efforts. But thanks for the question.

Anja: Thank you, Anne. We now turn to Senator Sam Nunn. Senator Nunn, are you with us?

Sam Nunn: Yes, I'm trying to unmute. Have I succeeded?

Anja: You have. We can't see you, but we can hear you.

Sam Nunn: Anne, thank you for your outstanding career and for your current leadership and for the initiatives in the cyber area that I mean, the Biden administration's undertaken. And David, thank you for the excellent book, The Perfect Weapon and your leadership in journalism in this area. We at NTI have done several cyber studies unclassified, and we have basically focused on command and control and warning systems and whether we can develop red lines with the Russians and with the Chinese in particular.

But indeed all nuclear weapons states need red lines in these areas because the cyber interference with command and control and warning systems could lead to, David, the perfect storm in the nuclear arena in terms of mistake, blunders, miscalculations. So Ernie Moniz and I are calling for and have for several months, actually a couple of years, a mandated study by the president of the United States to the Department of Defense to basically do a fail safe review on the ways that we could get into a war by mistake or a nuclear use by mistake or accident, or blunder, same question would apply to all the nuclear weapons states.

But this could be undertaken unilaterally, and we could challenge the other nuclear weapon states do the same thing because we all have the same problems. And it also applies to new systems as we modernize our force. And of course the classified world has got even more problems, I'm sure, but we've stayed in the unclassified arena. So Anne, I would hope that you all would consider and the Pentagon would consider undertaking this kind of fail safe review on new technologies, particularly cyber, but not limited to cyber and all the ways we could end up with a catastrophe.

There is some precedent for this back in the late '80s and early '90s basically got with Dick Cheney who was secretary of defense and asked for a review which wasn't on cyber then but it was on fail safe type review on the lack of attribution for submarines that could be mistaken for one country attacking the Soviet Union, the United States thinking it was the other. And that review was carried out in a very highly classified study but it resulted in a tremendous improvement in some of the fail safe procedures.

So I would hope that we would take a look at that and undertake that kind of fail safe review as well as challenge all the other weapon states to do so. Out of that, it would be my hope that countries with nuclear weapons would recognize that we have to have red lines in this arena. We cannot have the wild west in nuclear command and control and warning systems. So anyway, the question is, I know you all are looking at everything and I hope this is on your list.

Anne Neuberger: Thank you very much for the question Senator Nunn and thank you for just the leadership. You're an example for my generation of individuals to look at in terms of impactful work in this space. Certainly the introduction of new technologies brings new risks and we have to consider and certainly the networks we are always focused on with regards to risk are those command and control networks of our most strategic capabilities. So this is certainly an area of focus and consideration and appreciate the recommendation on that space.

Sam Nunn: Thank you.

Anja: Thank you. Anne, I wonder if we could rely on... Could we go five minutes over or do you have a hard stop?

Anne Neuberger: I think we have probably another two, three minutes, absolutely.

Anja: Perfect. We'll be very quick because I'd like to get to Bob Hormats who's backstage, virtual backstage and then to Munish who works on this from the New York city perspective. So Bob, turning it to you. Bob, are you there?

Bob Hormats: Thank you very much. Yes. Anne, thanks very much. I appreciate the conversation and I'd like to turn this a little bit to something David and I have discussed before, and I know Anne is dealing with as part of her overall responsibilities, and that is 5G. Currently we're very dependent on equipment and technology made by other countries. And the question is how much access their governments have to the equipment that is made in those countries.

My suggestion, and I wonder if the administration is looking at this, is that there are other ways of doing 5 and 6G technology that are based on more open systems, based on O-RAN. And a lot of American companies are exploring this. So you don't need first-generation equipment, you can use modern equipment of the second generation, which particularly includes new kinds of software, the cloud, silicon and other kinds of devices that can be used by any apparatus not just ones that are connected to those of other countries.

So I'm wondering if an open system based on O-RAN is something that you're considering and would consider. I think it helps our security. It's done by American companies, not foreign companies and it would be a big step forward to giving America a lead in 5G rather than where we are now, which is that we tend to follow the equipment and the technology of other countries. Can we do this? Are we doing it? And would you be inclined to take the lead in doing it to a greater degree with more companies, a wider group of companies than today?

Anne Neuberger: Couldn't agree with you more. And this has been a key focus area for us and the administration in the first few months, open ran. So for the broader group, 5G is important because it's the next generation of the internet, right? And not only does that reflect communications, it reflects can we have a global internet that reflects the values of civil liberties, privacy, protection from broad surveillance. That's so core to who we are as a democratic country with democratic allies as well.

And that's why we've put tremendous efforts to say, "What can we do to incentivize the build out of open ran, open standards based 5G approaches, which not withstanding the national security benefits have huge economic and innovation benefits as well?" Because instead of one black box end to end system, you have the opportunity for software based innovation at every level. It's been a big focus area, we've done active engagement with companies.

I gave a talk to the O-RAN ALLIANCE just last week. It's been a big part of our quad initiative as well with key countries as well given the need for security at 5G. So a lot of progress in that area, I think in understanding some of the incentives. And in addition, there have been pilot efforts across the US government that have really built out some open ran implementations and are making progress on that building on companies leading in this space, both in the US and Europe, and frankly, Japanese and potentially Indian companies as well. So a lot of innovations starting to spark in the space that we're excited about, and we hope to see the fruits up in the next year or two.

Anja: Thank you Anne. And just very quickly from Munish Walther-Puri who I think runs cyber risk for the city of New York.

Anne Neuberger: Thank you Anja.

Anja: Munish?

Munish Walther-...: Hello. I'm trying to turn on my video, but I'll just go with my... There we go. Thanks. Hi, my name is Munish Walther-Puri, I'm with New York City Cyber Command. Thank you for the extra time Anne, for answering my question. Can you describe some of the innovative ways you have seen or would like to see public private partnership in protection of critical infrastructure? Thanks.

Anne Neuberger: We always have time for people like you who roll up their sleeves that are part of doing the hard work of cyber each and every day and New York City Cyber Command has been a great example of innovation, public, private partnership and just really creative work. So thank you for the work you're doing Munish. I think you've seen a couple of good examples in the administration's work.

I mentioned the industrial control systems initiative, which worked closely with the Electricity ISAC, the information sharing public private partnerships established under the Department of Homeland Security critical infrastructure authorities. And the way we use that to really drive uptake of cybersecurity technologies across electricity systems and a key utility is that service as we talked about 90 million Americans, those efforts are now going to natural gas pipelines, to water and to chemical sectors as well.

So that kind of bringing in leaders in the sector and really providing them classified briefings to have them understand the threats, have them understand the need, I think the work in the executive order that outlined some very specific initiatives rather than saying, "Do it all," we said, "These are five things that would really have impact." And I think finally the work that we did in responding to the Microsoft Exchange hack and really bringing companies into the government's unified coordination group.

So those elements of focused purpose-built information sharing, focused on outcomes, practical rollout of technologies, sharing practical information that provides insights, but also frankly, listening and enabling the sectors to really address what's common about them, but what's distinct about each sector as well. And I think as we've looked at across utilities, across finance, across food safety, different approaches have been used, there are some commonalities, but that really affect, that really address the existing regulatory approaches, but also the key threats that face those sectors.

Anja: Anne, thank you very much. That was a masterclass. The country is very lucky to have you in this key role at this important time. We really appreciate you being with us and all the hard work that you do. And that was also a perfect segue because we're now going to hear from industry on what they are doing.