Fireside Chat

Moderator:


Speakers:

Sen. Joni Ernst, U.S. Senate, Iowa

Hon. Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology

###

Ellen Nakashima:

Good morning everyone. It's a thrill to be here today with two more illustrious and accomplished women than I could imagine, I'm honored. To my immediate left is Senator Joni Ernst, as you know, a member of the Senate Armed Services Committee, and the Ranking Member on the Emerging Threats Subcommittee, and the first woman combat veteran to ever be elected to the Senate. Awesome to see you and have you here.

Sen. Joni Ernst:

Thanks.

Ellen Nakashima:

And next to Senator Ernst is Anne Neuberger, the first ever Deputy National Security Advisor for Cyber and Emerging Threats we've ever had at the White House. And as part of her portfolio, she has made a focus of strengthening the relationship between government and industry and the private sector, especially in the area of innovation, both in the US and with allies and partners. So I think, though we have only 20 minutes, this should be a rich and lively conversation. And I think it's appropriate that we're doing this in Women's History Month because these two women are making history every day, not just every month. So it's, every day, Women's History Day. Alright, let's start here with Senator Ernst. As we sit here today, five months into the fiscal year, US war fighters across the world are being trained and equipped on last year's budget and a continuing resolution, the third year in a row that DoD is operating on a CR, right? And Congress is only now getting around, maybe, to passing this year's budget, never mind
Fiscal 2025. Senator, how are these budget battles affecting efforts to modernize the defense base and spur innovation, and what can be done to get your colleagues on the Hill to move faster?

Sen. Joni Ernst:
Yeah. Thanks Ellen. Next question.

No, and thank you, Ellen, for bringing this to the forefront because as we all sit here, yes, there is a lot of work that is going on on the Hill right now, and we do have very high hopes that this current fiscal year's appropriations will actually get done. What I understand is that they're busy in the House right now with the language, we anticipate it will come to the Senate on Friday. Now, if we are able to compress the time, we could actually take a vote on Friday. So we are hoping to get it done, again at the end hour before a shutdown. But you raise the important issue of the continuing resolutions, and every single one of you in this room knows how harmful continuing resolutions are to our military. We're not able to engage in new starts, new programs, certainly holding us to a previous year's appropriation is not helpful when we have an ever increasingly dangerous world. So let's all agree that it's harmful, and let's get back to regular order. That's what we need to do. But again, we hope to have this year's approach done on Friday. And then for heaven's sakes, we need to get next year's -- fiscal year's appropriations done before the fiscal year actually happens.

Ellen Nakashima:
Okay, great. Ms. Neuberger, the NSIB report card shows that China is closing the gap on emerging technologies like 5G and 6G. In fact, despite lobbying efforts by the Trump and Biden administrations, Huawei is still the world leader in 5G market share in the global South. China significantly subsidizes the cost of the gear. How do you deal with that, and are you changing your approach to competing with China in telecoms, especially in emerging markets?

Hon. Anne Neuberger:
So there's really two aspects to your question that I want to talk about a bit. Thank you, Ellen. One part is strategic technologies like telecom. And why is telecom so critical? Because the nation's secrets and the nation's IP ride on telecom networks, and the future of a number of industries, whether connected cars, whether UAVs, monitoring distributed energy infrastructure around the country to make maintenance or repair of down lines more efficient and rapid. All of that relies on connectivity and on trusted connectivity. So that's the reason that both the Trump administration and the Biden
administration have put such a focus on saying we must have trusted telecom. What makes China – and specifically Huawei, but really the two go together – such a potent competitor, is the fact that China maintains a largely closed market. Chinese, Indian, and US domestic markets are the largest telecom markets in the world.

And because China largely maintains a closed domestic market, they can subsidize their international subsidies by their domestic market. And Chinese products are good. The R&D budget of Huawei is twice Ericsson and Nokia, which are the two Western telecom equipment providers, are twice their budgets combined. So that really makes the Chinese industrial strategy, and notably Huawei, such a potent competitor. So the approach we've been taking, really building on the prior administration, the prior administration raised a great deal of focus on the need for trusted telecom. The answer we would often get back is, but you don't have an economically viable approach, right? Because of heavy Chinese subsidies, trusted telecom approaches were often 30 to 40% more. So what we've been working to do is bring the two parts together, the national security message with an economic package. And the first example of that has been Costa Rica.

In Costa Rica, one of our most trusted allies in the South, a host of the Summit for Democracy, one of the co-hosts, President Chaves, really following when he came into government, the country faced very significant – at the time it was a ransomware attack against government systems. Essentially Costa Rica's government systems were shut down. And it raised his awareness about the need for trusted digital infrastructure in Costa Rica. And as they were doing their 5G tender, they started working with the US government to say, how do we ensure that we can incentivize trusted vendors? So the US approach has been a combined three parts. Part one was a $25 million cybersecurity grant for Costa Rica to stand up a security operation center. That will become a regional security operation center. We'll be cutting the ribbon on it next month. The second piece, the first ever $300 million EXIM financing grant for trusted infrastructure. Exactly. Thank you. In Costa Rica. So bringing together the finance and our trusted goal. And the third part of that has really been investing in Costa Rica. We're lucky there's a strong, to your point, private sector base. Intel Corporation has a major place. There are other companies investing many call centers in Costa Rica. And indeed, next month, Costa Rica will be hosting a forum for 10 other regional countries to learn about their approach to trusted telecom. The US will be there with DFC, with EXIM, with our financing on the table, ready to discuss specific packages taking the Costa Rica model to a broader set of countries in partnership with Costa Rica.
Ellen Nakashima:
So staying on the theme of competition and emerging threats, Senator, threats to critical infrastructure involve not just attacks on power grids and oil pipelines, but on businesses, right? Especially small businesses that support innovation and modernization. How concerned are you about -- I know Ms. Neuberger works on the cyber angle a lot, but about acquisitions of these innovation companies by investment from adversaries like China, or efforts by these US companies to work in adversarial countries, and what are you doing about it?

Sen. Joni Ernst:
Yes, thank you, Ellen. I have a unique opportunity to be the Ranking Member, not just on the Subcommittee for Emerging Threats and Capabilities, but also the Ranking Member of the Senate Small Business Committee. And this is where we have seen our adversaries come in through the use of shell companies and other types of organizations that will use our existing programs through the federal government to gain access to grants and those small businesses. So we have various programs like the Small Business Innovation Research program. We have the Small Business Technology Transfer program. All of those are meant for American small businesses. They provide grants and opportunities to develop technologies that would be used by our Department of Defense. But what the Chinese, and again, other adversaries have been able to do is tap into those various programs and really use our own research dollars, our own grant dollars to take our innovation.

So in 2022, I did have a measure that passed that would prohibit any of our dollars going through SBIR, SBTT to our foreign adversaries. So we have the efforts in place now, but we have to really pay attention. Again, they can use shell companies and other types of organizations to tap into those dollars. So it's really important that the SBA do their homework as well through those programs and make sure that we are screening very carefully to make sure that we are not sending our taxpayer dollars to China, nor allowing them to access the innovation that's developed through these small business tools. So we are putting measures in place, we just have to make sure that we're enforcing them.

Ellen Nakashima:
Okay. Do you need to give them more authorities to plug these loopholes?

Sen. Joni Ernst:
We have the authorities now in place. And it’s very similar to situations you have in any of our agencies, whether it’s the Small Business Administration, whether it’s the Department of Defense -- anytime we’re pushing new authorities out there, we have to make sure that those within the agency that have the opportunity to administer those authorities, that they’re properly trained on the screening and how to use those authorities, and then actually does use them. So many times -- I’ll use the DoD as an example. There are a lot of authorities, especially in acquisition, to acquire new tools, new products. Many of those in acquisition, they’re afraid to use those authorities, or they don’t want to assume the risk to take on those new products. So again, we have to modernize the way we do business, but we have to hold those agencies accountable as well and make sure that the staff is properly trained to execute those new authorities.

Ellen Nakashima:
Right. And Ms. Neuberger, you’ve spearheaded initiatives to make critical infrastructure more resilient across industries. When it comes to the US military, recent revelations about Chinese government intrusions into, say, assets on Guam, and in Hawaii, and ports on the West Coast have raised real concerns. What is the administration doing – quickly, if you can say, because I know you’re doing a lot, but briefly -- to better secure these assets and how much of that effort depends on an ability to compel – not ask, not induce or incentivize, but compel the private sector to take these risks seriously through regulation?

Hon. Anne Neuberger:
So as you note, and you’ve written about this quite a bit, Chinese doctrine really sees the value of cyber, electronic warfare, space in bridging the vast regions of the Indo-Pacific. In both disabling potential military platforms, precision targeting, all the way through to disabling or disrupting the critical infrastructure that we deploy from in the United States. Our service members deploy from the same ports. The water servicing our bases is the same water we use regionally. So our critical infrastructure is key to the ability of the US to project power. I think what we learned following the Colonial Pipeline ransomware attack, and any number of other attacks, is that while voluntary standards have existed for a decade, many companies that operate -- own and operate critical infrastructure have not implemented them. So the administration has made a big push to really use either emergency authorities that each sector may have or to expand safety authorities to ensure that the owners and operators of critical infrastructure are locking their digital doors.
And we're talking about the basics we've been talking about for 10 years: encrypting data, passwords are dead, putting in place multifactor authentication. Because it is -- I've worked, I've had the privilege of working both offense and defense. It's a lot easier to be an attacker than a defender. So at the very least, doing the basics to lock our digital doors is needed. So that's been piece number one, making ourselves a harder target. The second piece of that has been setting rules of the road with various adversaries to say that an attack, a cyberattack on critical infrastructure would be treated the same as any attack on the homeland. Cyber is not something different. If you've disrupted our digital infrastructure that underpins our economy, it underpins our national security, that will be escalatory and will be treated in that way. And the third part of that has been truly building and deepening existing bilateral, multilateral partnerships.

So in the Indo-Pacific region, we have far -- now deeper cybersecurity partnerships with Taiwan, South Korea, the Philippines, Japan. Both individually and -- for example, the president hosted a trilat of Japan -- Japanese and South Korean leaders to bring those two countries together. So a number of those partnerships truly focused on both cybersecurity and the security of emerging tech are bearing fruit, both in the intelligence cooperation and in recognizing that the more secure we are, the more we can deepen intelligence sharing, the more we can deepen sharing of sensitive R&D technology. So having confidence in each other's digital infrastructure is the first step to the same kind of deeper partnerships we need in a potential Indo-Pacific crisis or conflict contingency. That was fast, I hope.

Ellen Nakashima:
That was really great. I have so many questions, but I just want to really get this one in for you, Senator. The Houthis are holding global shipping lanes at risk in the Red Sea with asymmetric warfare. We're spending millions of dollars to shoot down drones and missiles that cost tens of thousands of dollars. We're behind the cost curve in intercepting these missiles. What should we do? Strike Iran proper? Strike the supply chain as parts move through Oman or interdict them at sea? Or do we need to fight fire with fire and build cheaper drones at scale? What do you think?

Sen. Joni Ernst:
I think there are several options there without directly going after Iran, although we've had many people publicly say that perhaps that's an avenue someday. But yes, we need to make sure that we are preventing the opportunity to have those supplies coming out of Iran and going to the Houthis. I would throw China in that category as well, or even Russia. But preventing them from being built in the first place is really incredible. But it's
very difficult to do that. So we have to be able to counter their measures. And how do we
do that as well? We do engage. If you look at Task Force 59 in Bahrain, we have
opportunities there to test new technologies that would be much cheaper in the long run
to interdict the Houthis. Whether it's their ships, whether it's their rockets, their
technologies, identify it, reverse engineer it, and figure out how to counter it.

But we have to do it cheaper and we have to do it faster. That is key. What I hear a lot
from, yes, my constituents in Iowa as we are looking at how we are interdicting drones
or UAS, whatever it might happen to be – even interceptors that we see in Israel with
rockets coming in from Gaza – is why the heck are we spending $50,000 on an
interceptor to shoot down some little drone that's out there that our adversaries are
popping up and it's oftentimes commercial off the shelf? So we've got to figure this out
and be much more efficient with our taxpayer dollars, and they have to be more
effective as well. So that is our task, not necessarily sitting in the role as Congress, but
certainly as we're looking to all of our good friends here in the audience, those that are
engaged at DoD, those that are engaged in industry, we all need you to produce what we
can use effectively, but at a much, much lower cost.

We were just talking about the budget. I hate to talk about it in front of a lot of folks, but
we do operate in a constrained environment when it comes to the budget. And if you
look at what President Biden has proposed for next year, folks, we're being hamstrung.
So if we really do want to protect our homeland and project forward, and do it in a
manner that our taxpayers will approve of, then we've got to use our dollars much wiser.
So that would be my challenge to industry, to our partners at DoD, is let's find a way to
counter some of what the Houthis are doing in an inexpensive way. Let's find a way to
bolster our friends in Ukraine and in Taiwan with the most effective platforms that can
be done in a cost-efficient manner. So that's our charge right now. We don't need the
most exquisite platforms to counter the Houthis, but we certainly need a heck of a lot of
stuff that is much less expensive.

Ellen Nakashima:
Okay. I just wanted to get a quick question in on artificial intelligence. We talk about
emerging technologies – I know, and look, Senator Ernst, you know both Israel and the
United States are relying on AI to help Israel find targets for airstrikes. Israel has also
used drones to map out Hamas underground tunnels where the hostages are reportedly
held. In your opinion, is the department moving fast enough to get these AI tools fielded
in other combatant commands, other regions?
Sen. Joni Ernst:
Well, I would say, and just because we are running out of time, I'll try and keep it very brief. I would say that the Department of Defense is working very well with our industry partners -- with our industry partners to project AI forward and enable our friends in Israel and Ukraine. I'm terrified by AI and at the same time really excited about AI. We see it everywhere today and we don't realize it's out there. But what I can say is like SOCOM, and I see great friends from SOCOM here in the audience, they now have a multi-year contract with Palantir to work on AI in Ukraine, Israel, and elsewhere. And it allows us to take so much information through their large language model, take all of that information, just scrape the internet, get that info, put it all together, it saves a lot of our human capital and then narrow it down to the most important pieces in determining targets and so forth. So I'll stop there, but man, it's so exciting. There is so much we could do in the AI space.

Ellen Nakashima:
Okay. And I'm getting the stops, but last question I have to get in --

Sen. Joni Ernst:
I know you could go on forever.

Ellen Nakashima:
For Anne: how is the government seeking to ensure that adversaries are not using AI for purposes of war? Real quickly, in 10 seconds.

Hon. Anne Neuberger:
So – the New Yorker in me will come out. So here's what I would say: In the example that the Senator gave, AI demonstrates both the power and the risk. Because when we look at drone swarms, the opportunity to actually prevent them by shooting each one down or via interceptors, we can't. But adversaries using AI to locate our targets, potentially in a large sea, by target identification, and then rather than using GPS to navigate – but again, use the surface of where they are to find a target is a major risk. On the promise side, there are more efficient ways also to defend on that side. So I think the call to action for us, exactly as the Senator said, is to use the data stores we have. Build the models to ensure that AI driven defense is always a step ahead. And notably in the arenas, both of defending military targets that are deployed as well as in the arena of cybersecurity, where amassing data can make a difference in speed.
And the speed of finding an adversary who has exploited your network is key, because the faster you can find and push them out, the more you can manage the harm. So those are two areas where across the government there are active efforts underway between DoD and the intelligence community, and notably a real call to action on a lot of creative work coming in from the private sector that I think will really move the needle far faster than in many cases the Department and government would do on its own. So a thank you for that partnership, and it's really the call to action in the four words on the wall right there.

Ellen Nakashima:
Alright, thank you very much Deputy National Security Advisor Neuberger and Senator Ernst. Give them a round of applause. Thank you.

###