U.S. Senator Maria Cantwell
Telecom Subcommittee Hearing "Intelligent Networks: Powering Artificial Intelligence and Transforming Communications."
July 30, 2026
Sen. Cantwell Q&A
[VIDEO]

Sen. Cantwell: Thank you, Madam Chair. Thank you so much to you and Ranking Member Luján for holding this important hearing and your continued focus on these important communication issues. I want to thank my colleague from Indiana who just spoke about how this is a national security issue, and he and I worked on the first federal role for our government in AI policy and got that implemented. And every day, I am thankful that we got that started, I think…it's probably six years ago. But anyway, we are here today -- and we continue to see a fast-moving environment -- and the question is, what are we going to do to step up to that, both from the security point of view and from a competitive point of view.

So, artificial intelligence. We saw last week with OpenAI's disclosure of an unprecedented security incident -- one of its advanced models broke out of the sandbox and created a complex cyberattack against Hugging Face. AI can design viruses, toxins, biological weapons that can be used to design entirely new pathogens that are difficult to detect and counter. And today's hearing comes at an important moment as AI accelerates new capabilities that are being unlocked every day. But we still need to compete.

So, Mr. Ramzanali…you brought this up in your testimony about the Hugging Face [incident], making it abundantly clear that we needed to have regulation on these -- not self-certification -- but some regime. And that it might often need us to look into this from an international perspective too, because we're not just regulating this technology for what might happen in the United States, but what malign actors might do with this technology as well. So, what do you think that we need to do to make sure that we get this right?

Particularly, I think this committee knows a lot about cybersecurity. I think over the time I've been on the committee we've had many, many hearings about cybersecurity. It's a whole-of-government response with many different agencies and we continue to see attacks on the private sector, telecom sector -- ill-prepared to respond -- and we also saw it on our pipeline system. This makes that look like child's play.

So, could you elaborate on what you think we need to do to address issues like the biological threats, where AI can provide step-by-step instruction for engineering of novel, resistant, supercharged super bugs -- it could just go off and do that. The advanced AI models could be really key in solving some very important [problems], but also could be used for uranium enrichment and nuclear bomb trigger designs. And so, if that gives a lot of people on an international basis access to more information and proliferation, what do we do about that?

And then just on this cybersecurity model, again -- very familiar coming from a very big software state -- we all know that software can be buggy. But now, we're not talking about buggy software. We're talking about software that writes itself, goes and attacks systems, creates big

holes. It's almost like it's a chemical itself in the kind of damage that it could be doing corrosively within our cybersecurity network and we wouldn't even know about it.

So that's a lot, but we invited you here because we thought you could help us with this. And what are the things that we need to put in place?

Mr. Ramzanali: It's a lot, but this is the core of the problem. So I appreciate you highlighting it and your longstanding work on these issues. I think about this in a few different ways. First, all of the critical infrastructure systems that we have today need to be hardened. Second, pre-deployment testing can help us become aware of the types of threats that are coming and this is the role of government. Government has biologists, it has nuclear weapons experts. The national labs that we employ have those kinds of experts. We should be deploying all of them to help understand what the threat landscape looks like. Third, each one of those threats that you described has its own supply chain and ecosystem, and we need to look at it from a systems lens.

When we talk about the biological concerns that you raised, there is a question about what are models able to do. What does that look like when you're able to do one exploit after another? But there's also a whole host of other things that have to happen, including integrating with cloud labs, getting access to biological agents. So we should be looking at every part of that, and I'm worried that we're not looking at every part of that and doing as much as we can. Both the last administration and, to its credit, this administration have made progress on some of these questions, but we have to do way more, I think you're exactly right to say that the landscape is changing and we're still moving incrementally in some of these domains.

Sen. Cantwell: We shouldn't be fearful about these national security organizations within our government being involved in trying to get this right and protect us? Is that correct? I think some people are proposing there's like this self-certification model and we just have to go fast. I think what we have to go fast on is all of us coming together on what are the right security layers to protect our citizens and our nation and to advance our competitiveness. And so that often does take some of the smartest people within our federal government, particularly when you're dealing with some of these biological or nuclear weapons.

Ramzanali: That's exactly right. The scale of the problem we're talking about, when it relates to safety and security, is not commensurate with a self-certification voluntary regime. We don't put up with massive safety and national security concerns with paperwork being the response in any other domain.

Sen. Cantwell: Well, it certainly hasn't worked out in aviation I can tell you that. We're just advancing too fast, if you ask me. Even in aviation…you are trying to understand the interaction between hardware and software. But in this case, I think that what hasn't been amplified is how dangerous the cyberattack universe is—just that in and of itself -- and how promulgating, I guess is the right word -- I'm not sure that's the right word but I'm going to use it—promulgating of the attack that AI could be, it could be quite significant on its own, you know, going through a system.

Ramzanali: It would be incredibly disruptive to our lives if we have to consistently worry about AI-based cyberattacks disrupting banks and hospitals and telecommunication systems, because that's just happening as a regular part of our life. We should not accept that future. We should try to avoid a future where those kind of attacks become commonplace.

Sen. Cantwell: And what, well, I don't think we've quite got the cyber regime correct yet today, because we are still seeing attacks and a lot of personal information still being exposed, and I think we continue to want to work with our telecom industry to make sure they're making the investments that keep us going. I see I'm over time Madam Chair can I go on one more question? [W]hat areas do you suggest we engage on an international basis to get an international regime? What areas would you suggest?

Ramzanali: The international part's the hardest. That's where there's going to be diverging interests that we have to figure out. One of the oldest existing international organizations we have is the ITU, which started as the International Telegraph Union, because we needed to come together to figure out a system that works for a technology that doesn't respect borders. That's where we are today, and the threats are much bigger, and the issues at play are much larger. We do have to figure something out. There was a lot of work done in the last administration. This administration is doing a lot. All of those feel insufficient. So I think we need to rethink how we approach this and start from: what are everybody's interests? And I do believe there are shared interests in safety and security.

Sen. Cantwell: I agree, but I think we have to think about some of these non-proliferation regimes that existed and how they functioned, and what we have to do here as well. And so we'll look forward to more questions. But thank you for this very important hearing. Appreciate it.