REMARKS OF FCC CHAIRMAN AJIT PAI
TO THE CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

JANUARY 5, 2021

Good afternoon, and happy New Year to all of you.

Thank you to Dr. Hamre and everyone at the Center for Strategic and International Studies for welcoming me today. This is my first time speaking to CSIS, and, as far as I'm aware, the first time an FCC Chairman has spoken to CSIS in a quarter-century. In his 1996 remarks, Chairman Hundt lamented a world where two-thirds of the population had never made a phone call and half of all people lived a two-days walk from the nearest phone. Considering that we now live in a world where there are more cell phones than people, I think it's fair to say that it's been too long since an FCC Chairman addressed CSIS.

There's another CSIS connection to the 1990s, this one more personal. In the fall of 1990, I took what became one of my favorite classes as a Harvard undergraduate. It was Historical Study A-12, "International Conflict and Cooperation," taught by Joseph Nye—who also serves as a CSIS trustee. The class focused on the study of conflicts, from the Peloponnesian War to World War I. One thing that sticks with me even now is how often governments seemed to misunderstand, or miss entirely, the nature of the threats they faced. As a result, frictions became conflicts—often quite destructive ones. Because of that course, I became convinced that governments should actively wield hard and soft power, as appropriate, to navigate nations through the turbulence of the times.

Now, I certainly didn't anticipate that I'd be in a position to incorporate lessons from Professor Nye's class three decades later. But that has been a key part of my job at the FCC. The Communications Act of 1934 outlines several reasons why our agency was created, including "for the purpose of the national defense" and "for the purposes of promoting safety of life and property." Consistent with those charges, identifying threats to our communications networks and taking aggressive action to counteract those threats have been among the hallmarks of the FCC during my four years as Chairman. With communications technologies underlying virtually every aspect of our economy and society, and with the pace of technological change quickening, it's become more important than ever that government be proactive. And that we have done.

To understand how far we've come, it helps to describe where we started. It seems like ancient history in a time when a week feels like a year, but the United States government's orientation toward geopolitical threats and the FCC's orientation toward national security were entirely different before I came into office. To give you a sense of the former, the official position of the U.S. government during the previous Administration was that the United States "welcomes the rise of a China that is stable, prosperous and peaceful," and that "our two great nations, if we work together, have an unmatched ability to shape the course of the century ahead."

As for the previous FCC, it allowed federal subsidies to be used by U.S. telecommunications carriers to purchase equipment from companies with close ties to the Chinese Communist Party and military, like Huawei and ZTE. And it issued a non-binding white paper on cybersecurity—on January 18, 2017, two days before Inauguration Day—that had no concrete plan of action and didn't mention China at all.

Things are different now—much different. If there is one thing most people across the American political spectrum agree on today, it's that China presents serious challenges to the national security of the United States and our core values. That feeling is shared by the American public, not to mention a growing number of people around the world. In a 2020 survey of those living in 14 nations with advanced economies, a majority of people in every country had an unfavorable view of China. In all 12 countries with historical data, the unfavorable rate had increased over the past year, with a spike as high as 24 points in Australia, where 81% of residents now have a negative opinion of China. In the U.S., the

percentage of people with an unfavorable opinion of China increased from 60% to 73% over the past year.

Where does this global shift in sentiment come from? A lot of it, no doubt, has to do with the many examples of the Chinese Communist Party's appalling behavior, from the repression and detention of Muslims in Xinjiang to the crushing of dissent in Hong Kong to corporate espionage and rampant theft of intellectual property to the concealment of the COVID-19 outbreak that has had a catastrophic impact across the globe.

But there is also an increasing recognition that the Chinese Communist Party is using its growing influence over global commerce to advance its own pernicious interests. Just three weeks ago, for example, Zoom's liaison with Chinese government officials was charged by federal prosecutors for disrupting and censoring video meetings commemorating the anniversary of the Tiananmen Square massacre. And last month, we saw two new reports linking major Chinese companies to the government's persecution of Uighur Muslims. Documents were uncovered revealing that Huawei had tested facial recognition software that could be used by China's Orwellian surveillance system to identify Uighurs, which would trigger automatic alerts to local police. And Alibaba, sometimes characterized as China's version of Amazon, was caught marketing the ability of its cloud services to detect the faces of Uighurs and other ethnic minorities.

These cases reflect a disturbing and growing pattern of behavior by China. They also raise a broader concern about the security of the United States. If China is willing to use its business connections and leverage to shut down online memorial services, who knows what would happen if we allow Chinese companies' equipment to be incorporated into our communications networks.

So whatever our policy differences on other matters at the FCC over the past four years, on this issue we've had a consensus. We've acted decisively and in a bipartisan way to address the threats to our communications networks.

Take the issue of supply chain integrity. For years, U.S. government officials and national security experts have expressed concern about the security threats posed by certain foreign equipment and software providers. Hidden backdoors to our networks in routers, switches, and other network equipment can allow hostile actors to inject viruses and other malware, steal Americans' private data, spy on U.S. companies and government agencies, and more.

This threat is compounded by the consolidated marketplace today for advanced communications equipment. Indeed, the largest global supplier right now is the Chinese company Huawei. This is a major concern.

While Huawei positions itself as a private company, it has significant ties to the Chinese government, namely, the Communist Party and China's military. Moreover, China's National Intelligence Law requires all companies subject to its jurisdiction to comply with requests from the country's intelligence services. These requests cannot be disclosed to any third parties, such as Huawei's customers in China or abroad. That means China could compel Huawei to spy on foreign individuals and businesses and prevent Huawei from disclosing such surveillance requests. And this isn't just hypothetical: Independent cybersecurity experts have found numerous backdoors and other vulnerabilities in Huawei equipment and firmware that put private information carried by that equipment at risk.

At the FCC, we have taken action to address this threat. Specifically, we have prohibited the use of money from our over $8 billion a year Universal Service Fund to purchase or obtain any equipment or services produced or provided by companies that the Commission determines pose a national security threat to the integrity of communications networks or the communications supply chain. And we have specifically designated Huawei and ZTE as companies that pose such a threat.

We also recognized that some U.S. carriers had already incorporated insecure equipment into their networks. So we had to come up with a process from scratch for addressing this problem—and we did. We started a data collection to identify and catalog insecure equipment used in USF-funded communications networks. Having completed this review, we determined that it will likely cost at least $1.8 billion to remove and replace Huawei and ZTE equipment in U.S. networks. We adopted rules to implement the so-called "rip and replace" program, which will require carriers to remove this equipment and reimburse them for the cost of replacing it. And just last month, Congress provided the FCC with $1.9 billion for this program. So we are now well on the way to getting insecure equipment out of our nation's communication networks.

In addition to addressing the equipment that goes into our networks, the FCC has also taken action to ensure that foreign telecommunications companies that obtain or seek access to the U.S. market do not present a national security threat. In May 2019, the FCC denied China Mobile's application to enter the U.S. market for national security reasons. Since this decision, we issued orders to four other Chinese state-owned companies—China Telecom, China Unicom, Pacific Networks, and ComNet—that already hold such FCC authorizations. The orders required these companies to demonstrate why the FCC should not begin proceedings to revoke and terminate their authorizations to operate in the United States based on similar national security concerns. Last month, the Commission started the process for determining whether to revoke and terminate China Telecom's authority to operate in the United States. The FCC found that China Telecom has failed to rebut the serious concerns of the Executive Branch about its continued presence in the United States and that more than sufficient cause exists to move forward. We also recently received additional information and evidence from the Executive Branch on the security threats posed by the remaining three companies.

The Commission's China Mobile and China Telecom decisions followed recommendations made by expert agencies in the Executive, which concluded that the companies' operations in the United States pose substantial national security risks.

This is consistent with our overall "whole of government" effort on national security issues in the telecommunications sector. For example, last April, the President issued an Executive Order reforming the process by which the Executive Branch assists the FCC in evaluating national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector—what has traditionally been known as the Team Telecom process. And then last fall, the FCC adopted a new set of rules consistent with the Executive Order, formalizing the close working relationship across our agencies on foreign-ownership matters and offering much-needed clarity to the private sector on Team Telecom's operations. They also require parties to furnish Executive Branch agencies with responses to a set of standardized national security and law enforcement questions designed to provide the agencies with information they need from applicants to facilitate their review. Our reform of the Team Telecom process, which facilitates beneficial foreign investment and prevents harmful foreign ownership, is a clear indicator that this broader effort is not about isolationism or protectionism; it's about allowing such investment consistent with national security.

Thus far, I've talked about the decisive action we've taken on what you might call "defensive" measures: preventing problematic equipment from getting into our networks, denying market access to problematic carriers, and the like. But we've also been on offense, too, to ensure that our nation's communications networks will enable us to be strong economically at home. There's perhaps no better example of that than 5G, the next generation of wireless technology.

These networks will bring exponential increases in speed, responsiveness, and capacity. They will enable new and improved services and applications that will grow our economy and improve our standard of living.

That's why the FCC has aggressively executed what we call our 5G FAST plan, which features three key parts: freeing up commercial spectrum, promoting the installation of wireless infrastructure, and

encouraging fiber deployment (fiber being critical for backhauling wireless traffic into the core of the networks).

This market-driven strategy has been incredibly successful. For example, we've completed four auctions in less than two years that have repurposed massive amounts of spectrum for 5G. And we're on the brink of wrapping up the highest-grossing spectrum auction in U.S. history, which will free up 280 megahertz of spectrum for 5G. In addition, we've seen an exponential increase in wireless infrastructure during my tenure, with ten times as many new cell sites deployed over the past four years as in the four years before that. And the U.S. set a record for fiber deployment in 2018, a record that was broken in 2019.

Leading the world in 5G development and deployment is critical for our economy and global competitiveness. But we've gone even further. It's not enough for our 5G networks to be strong. They also have to be secure. When 5G is embedded in almost every aspect of our society and economy—from businesses to homes, hospitals to transportation networks, manufacturing to the electrical grid—securing our networks will become much more important and much more difficult. And this has to be considered at the outset of 5G deployment. We simply can't take a risk and hope for the best.

As a Council on Foreign Relations white paper explained, "5G networks will expand the number and scale of potential vulnerabilities, increase incentives for malicious actors to exploit those vulnerabilities, and make it difficult to detect malicious cyber activity."

So in addition to the specific steps I outlined earlier dealing with supply chain integrity, we've encouraged companies to think about the network architecture of the future.

Traditionally, wireless networks relied on a closed architecture, in which a single vendor supplied the components between the network edge and core. Now, telecom companies have begun developing and deploying open, interoperable, standards-based, virtualized radio access networks. This is essentially software displacing hardware. These Open Radio Access Networks, commonly known as Open RANs, offer an alternative to traditional cellular network architecture. And they could enable a diversity in suppliers, better network security, and lower costs. And from a national perspective, we have an existing advantage in software development, and a culture that embraces open-source solutions.

The FCC has encouraged the research and development of Open RAN solutions. This past September, the FCC hosted a meeting of experts from the public and private sectors to discuss the current state of Open RAN-related technologies and the path ahead. A consensus emerged from the forum that Open RAN technologies are already showing great promise in the U.S. and around the world, and that the public and private sectors should continue to collaborate and help encourage their deployment.

We've also been on offense on the international front. I made it a personal priority to advance the cause of network security diplomatically, both through multilateral engagements and directly with our foreign partners. Indeed, I daresay that I've visited, spoken with and cooperated with our foreign counterparts more than any FCC Chairman in recent history.

Now, when this initiative started, pessimism was the dominant reaction here at home. There was much chatter here about how the FCC wasn't doing enough, how the U.S. government was going it alone, and how we were unlikely to get results—you name it.

But we stayed the course, and we succeeded.

The multilateral engagement has been especially fruitful. For instance, in May 2019, I traveled to Prague as part of the U.S. delegation for a high-level conference on 5G security with key international allies. That conference resulted in the creation of the Prague Proposals: a concrete, risk-based framework for understanding the security of communications networks. 32 countries, including the United States, agreed to that framework. The Prague 5G Security Conference redoubled its efforts this past September, holding its second summit (virtually) to address ongoing issues regarding vendors posing national

security threats, as well as the potential for Open RAN technologies to make 5G networks more secure. I laud this multinational effort not just for its substance but also for what it symbolizes.

For the FCC, Prague was a blueprint for what was to come. Ever since then, I've raised the issue of 5G security and supply chain integrity almost every time I've gone abroad and spoken to international audiences. There have been many: the United Arab Emirates, Bahrain, Saudi Arabia, India, Germany, the United Kingdom, Malaysia, Singapore, Vietnam, and Japan, to name a few. Sometimes I've made the pitch alone. Sometimes, we've worked with other agencies to advance this message. But the common thread is that we've built capital by demonstrating with our presence and voices and ears that we value our bilateral relationships on this issue.

For instance, two years ago, I briefed the State Department's Chiefs of Mission Conference—the annual meeting to which all leaders of U.S. diplomatic missions abroad are invited—on 5G security issues. This led to more information sharing with our posts around the world, positive exchanges abroad (such as a productive visit to Portugal, hosted by the U.S. ambassador), and more.

This work hasn't been easy. It's taken a lot of time. It's required careful diplomacy. And it's often been without immediate apparent effect. But now we are seeing the results of our work. And I'm pleased to report that the tide has turned significantly toward the U.S. position on 5G security.

Australia and Japan moved early to exclude Huawei equipment from their domestic communications systems. The European Union has adopted strict guidelines for vetting 5G equipment vendors, "allow[ing] EU capitals to limit Huawei's role in 5G networks across the Continent in coming years." A number of countries across Europe—including the Czech Republic, Poland, Romania, Denmark, Estonia, Latvia, Sweden, and Greece—have taken steps prohibiting these high-risk vendors from their networks. Of particular note, in July 2020, officials in the United Kingdom announced that they would reverse course and remove Huawei equipment from their 5G networks. India has taken significant action against Chinese mobile apps which they deem to present a national security threat. The momentum here is unmistakable and it is positive.

On top of that, communications providers in many countries have decided to limit or cease business dealings with problematic vendors altogether. For example, major providers like Telefonica in Spain, Orange in France, Telstra in Australia, SK and KT in South Korea, and Reliance Jio in India have cut Huawei from their mobile phone offerings, network cores, and future 5G network builds.

Of course, getting back to an earlier theme, it's important to emphasize that these efforts would not have been successful without a "whole of government" approach. I don't have time to mention here all of those who have contributed to this international initiative. But I would like to single out three individuals with whom I've had the privilege of collaborating closely on this issue: former Deputy Assistant Secretary of State Rob Strayer, Josh Steinman, Senior Director for Cyber at the White House National Security Council, and Robert Blair, formerly in the White House Chief of Staff's Office and now Director of Policy and Strategic Planning at the U.S. Department of Commerce. These three patriots have worked tirelessly to promote secure 5G networks and deserve far more recognition than they have so far received.

* * *

Of course, we will soon hand the baton to a new Administration. They will have to decide the approach that they are going to take to addressing the security of our communications networks. And I hope that they succeed. On this issue, their success will be our nation's success.

Of course, these challenges won't be easy for them, just as they weren't easy for us. But they have an advantage: the solid foundation we have laid for securing our communications networks, both here at home and around the world. It is a foundation that can be built upon to ensure that our networks remain strong and secure.

The other advantage they have is that there is now a bipartisan consensus on the importance of these issues, both at the Commission and on Capitol Hill. We can and must no longer consider foreign threats to be sufficiently addressed with aspirational talk, bureaucratic indifference, or a naïve approach to the world that simply pretends these threats do not exist. I am optimistic that there will be no turning back.

Finally, I will always be grateful to everyone at the FCC who helped make this progress possible. In particular, thank you to the staff of our International Bureau, Public Safety and Homeland Security Bureau, Wireless Telecommunications Bureau, Office of Economics and Analytics, Wireline Competition Bureau, Office of Engineering and Technology, and Office of General Counsel. And thank you to those in my office who have worked long and hard on these issues over the past four years: Rachael Bender, Matthew Berry, Nick Degani, Aaron Goldberger, Zenji Nakazawa, Nirali Patel, Sean Spivey, and Preston Wise.

I appreciate CSIS for hosting me today, and look forward to continuing to work with you and many others to build a brighter, more secure future for our fellow Americans.