# Opening Statement for Chair Cathy McMorris Rodgers Subcommittee on Communications and Technology "Securing Communications Networks from Foreign Adversaries."

**February 15, 2024** 

(As Prepared for Delivery)

### **INTRO**

Good morning, and thank you, Chairman Latta.

Over the past year, this committee has held numerous hearings to discuss the many threats posed by the Chinese Communist Party to the U.S.

These range from supply chain vulnerabilities to espionage and attacks on our communications networks.

# CHINA IS TARGETING OUR CRITICAL INFRASTRUCTURE

China-based companies, like Huawei and ZTE, have emerged as top players in the global telecommunications industry...

These companies operate in an environment tightly intertwined with the Chinese government, raising questions about their independence and potential for exploitation by the CCP.

Relying on their technology comes with significant risk.

It could be used by the CCP to surveil Americans, steal people's personal information, and even shut down entire networks.

Homes, schools, hospitals, our financial system, and the military are all in jeopardy as long as this equipment remains part of our communications infrastructure.

That's why in 2019, Congress enacted the Secured and Trusted Communications Networks Act to remove Huawei and ZTE entirely from our networks entirely.

That work is ongoing, and it continues to be a top priority of this committee to make sure carriers have the resources they need to remove this equipment from U.S. networks and replace it with trusted equipment.

But that's just the first step.

China's aggressive pursuit of technological advancement is a direct threat to American national security and economic leadership.

The Chinese government's strategic initiatives, such as the Made in China 2025 plan and the Belt and Road initiative...

...aim to achieve dominance in technologies that are critical to winning the future.

That includes technologies like artificial intelligence, quantum computing, and advanced manufacturing.

At the recent World Radiocommunication Conference, we witnessed this firsthand...

...as China and Huawei aggressively worked to undermine U.S. leadership on spectrum policy and give Huawei a global competitive advantage.

Additional actions taken by China, including intellectual property theft, forced technology transfer, and state-sponsored industrial espionage...

Further undermine free markets, fair competition, and American innovation and entrepreneurship.

### CHINA'S CYBER THREAT

Perhaps most alarming is the evolving landscape of cyber threats posed by China.

Last month, we held a hearing on cybersecurity, where we examined how foreign actors are increasingly exploiting widespread vulnerabilities in our critical infrastructure.

State-sponsored cyberattacks targeting U.S. government agencies, businesses, hospitals, and our military have become increasingly sophisticated, frequent...

...and pose significant economic and national security risks.

Look no further than the 2017 Equifax data breach, which exposed the personal information of hundreds of millions of Americans...

...or the 2020 SolarWinds incident, which gave China-based hackers access to sensitive information across the federal government.

These vulnerabilities must be addressed.

# **TODAY'S LEGISLATION**

Today, we will examine a number of legislative solutions to counter the influence of China and promote U.S. leadership in technology.

This hearing will be an opportunity to discuss adding certain CCP-controlled technologies and equipment to the Federal Communications Commission's Covered List...

...and how to increase transparency for Americans about which companies operating in the U.S. are owned by China.

We will also look at ways we can strengthen communications with our allies overseas and establishing a 6G taskforce to advance American innovation and win the future.

## CONCLUSION

The United States faces exceedingly complex threats from China and other adversaries that require a comprehensive and coordinated response.

This response must include efforts to secure critical supply chains, protect our allies, strengthen cybersecurity defenses, and engage in strategic competition with China in key technologies.

Failure to address these challenges effectively not only jeopardizes U.S. economic competitiveness and national security...

... but also risks ceding ground to an adversarial power intent on reshaping the global order in its favor.

I'd like to thank our witnesses for being here today and I look forward to this important and timely discussion.

Mr. Chairman, I yield back.