Chairman Mike Gallagher (R-WI)

Opening Remarks | The CCP Cyber Threat to the American Homeland and National Security | January 31, 2024

(As Prepared for Delivery)

CHAIR: In war, the enemy works tirelessly to sabotage critical infrastructure. It poisons water supplies, cuts power lines, and destroys dams. In short, it seeks to create societal chaos.

That is what the CCP is positioning for today across America. The only difference from wartime saboteurs of the past is that the PRC is doing it in cyberspace.

This is not conjecture. This is happening right now.

And this is nothing new.

For over 20 years, the CCP has been attacking us — our government, our defense contractors, our technology firms — in cyberspace.

For a long time, these attacks were focused on theft, robbing us of invaluable technology that was then used to drive China's military modernization.

Another focus of attack has been gathering sensitive information on hundreds of millions of Americans with attacks on companies like Anthem health, and the Office of Personnel Management.

According to the FBI, "China's vast hacking program is the world's largest and they have stolen more Americans' personal and business data than every other nation combined."

But that wasn't enough for the CCP. In the past few years, our intelligence and cybersecurity agencies have discovered that the CCP has hacked into American critical infrastructure for the sole purpose of disabling and destroying our critical infrastructure in the event of a conflict, likely over Taiwan.

This is the cyberspace equivalent of placing bombs on American bridges, water treatment facilities, and power plants. There is no economic benefit for these actions. There is no intelligence gathering rationale. The sole purpose is to be ready to destroy American infrastructure, which will inevitably result in mass American casualties.

These outrageous actions represent an active and direct threat to the American homeland and military.

This is not a hypothetical. As our witnesses will testify today, ***the Chinese*** government ***has already done it*** and our cyber warriors are doing everything they can to stop it.

Chinese hackers have put malware in water utilities, oil and gas pipelines, power grids, and other utilities in our westernmost territories and across the American homeland.

Just imagine the damage the CCP could inflict during a Taiwan invasion if with a flick of a button, they could close ports, turn off the power, and cripple pipelines throughout the United States, while cutting our military off from desperately needed fuel?

This is precisely what this "pre-positioning" makes possible.

We must heed Xi Jinping's own warning that "without cyber security, there can be no national security."

This is a ticking time bomb aimed at the heart of our economy and our national security.

The same grids that heat our home, underpin our economy, and provide our water also power ports and airports that our military relies on to respond to a crisis.

If the grid goes dark, so does our ability to fight and win.

It is time to wake up and recognize the full scope and scale of the PRC cyber threat to America.

This is not just a government problem. This is a whole of society problem.

It will take unprecedented collaboration between the public and private sectors to create the kind of layered cyber deterrence we need to prevent disaster.

Our committee is called the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party.

But in a very real way, the name of our committee vastly understates the problem set. This is not just strategic competition but a strategic ***threat*** pointed at the heart of America. If we do not address this threat, then the Chinese will have the ability to turn off the lights for everyday Americans, shut down entire cities, and cause a massive loss of American lives. That is unacceptable. We must address this threat before it is too late.