Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States"

Opening Statement of Commissioner Carolyn Bartholomew

February 17, 2022

Washington, DC

Good morning, everyone. Thank you for joining us today. Thank you, particularly, to our witnesses for the knowledge and expertise they are sharing with us. We look forward to learning from them.

In addition to cyberwarfare, this hearing will explore China's motivations and capabilities for cyberespionage. In contrast to cyberwarfare, which aims to infiltrate and compromise an adversary's computer networks, cyberespionage is a clandestine operation to access and steal classified or otherwise sensitive data for political or military purposes, or to illicitly acquire intellectual property to gain a competitive or economic advantage over an adversary.

In 2005, this Commission started raising concern about China's cyber activities. It was becoming clear that China's theft of intellectual property was moving from counterfeiting CDs and other physical goods to online theft of trade secrets. China's tradecraft at that time was ham-handed and relatively unsophisticated. Since then, there has been an alarming rise in the frequency and the sophistication of China's state-sponsored and state-affiliated cyberespionage activity, as well as its targeting.

China's cyber actors have deliberately and aggressively pursued targets across a spectrum of industries, including technology, defense, energy, healthcare, education, and other key sectors in pursuit of trade secrets and of sensitive information. One of the most recent and egregious, the Microsoft Exchange hack in July 2021, compromised email servers and consequently the sensitive information of tens thousands of organizations in the United States and around the world. In the healthcare sector, Chinese cyberespionage campaigns have targeted hospitals and research institutions for data that could confer competitive advantages in science and technology. In May 2020, the FBI disclosed that it was investigating "the targeting and compromise of U.S. organizations conducting COVID-19-related research by PRC-affiliated cyber actors and non-traditional collectors." Reported breaches of healthcare insurer Anthem Inc., Equifax, Marriott, and, perhaps most worryingly, the Office of Personnel Management, all demonstrate China's vast campaign to target and acquire Americans' private data through cyberespionage.

The threat of China's cyberespionage activities is not only a U.S. challenge, but also a global one which underscores the need for collective action and security cooperation with U.S. partners and allies. In July 2021, the Biden Administration affirmed that the United States is working with an "unprecedented group of allies and partners – including the European Union, the United Kingdom, and NATO" to address the threat of China's "irresponsible and destabilizing behavior in cyberspace."

Today's witnesses will provide insight into China's intent and capabilities for cyber espionage, and critically what the United States and partners can do to address this challenge effectively.

Finally, before we begin I would like to remind you all that the testimonies and transcript from today's hearing will be posted on our website, which is www.uscc.gov. Also, please mark your calendars for the Commission's upcoming hearing on China's energy policies and practices, which will be on March 17. I will now turn the floor back over to Chairman Wong to introduce our first panel.