Additional questions for the record from the May 16, 2018 Subcommittee on Communications and Technology hearing entitled, "Telecommunications, Global Competitiveness, and National Security"

Samm Sacks, Senior Fellow, Center for Strategic & International Studies

The Honorable Marsha Blackburn

1. **China and other competitors have explicitly stated their desire to dominate specific nodes in the supply chain. Given the global nature of the supply chain for information and communication technology, what is our risk?**

   There are espionage and economic risks. I leave it to the national security experts to determine the specific threat and how to mitigate it. However, it is difficult to comment on the threat because there is not publicly available information on it. More specific information should be made public so there can be a comprehensive analysis about how to mitigate the threat and what the impact of different measures would be.

   a. **If our competitors were to capture critical nodes in the supply chain, either through market share or through technical prowess, what recourse do we have?**

   The United States should not take a sweeping approach that blocks entire companies or discriminates against companies just because they are of a certain national origin. Our policies need to determine the impact of our actions on the U.S. economy, U.S. companies, and our ability to maintain technological leadership and innovate.

2. **It seems that the trusted vendor pool is shrinking each year. If this pace continues, we could find ourselves with only one trusted vendor providing communications infrastructure in the U.S. How can government and industry promote competition and longevity for trusted vendors in the market?**

   We must recognize the interdependency of technology and carefully assess the implications for disentangling the United States from global supply chains. Any measures taken against specific competitors should be coordinated efforts with allies and partners to exert international rather than unilateral pressure.

2. **As you note in your work, China uses a command and control approach to orchestrate their national strategies on the supply chain for information technology, emerging technologies, and R&D. The U.S. does not take such an approach; rather, we rely on market-based mechanisms. Can you elaborate on the advantages and disadvantages of command and control, and how the U.S. can leverage the strengths of its market-based approach?**

The Chinese government uses systematic efforts to bolster domestic industry by identifying certain sectors for state support (e.g., by direct subsidy, access to credit or special pricing or other preferential policy treatment). There is also a push for Chinese companies to have a major voice in shaping standards and to expand into global markets.

The semiconductor industry is an example of where decades of state support has not enabled China to develop an indigenous industrial base and reduce reliance on core foreign technologies. On the other hand, Chinese sectors like the digital economy (e.g., ecommerce platforms, financial technology, mobile apps) that are largely commercial and market-driven have demonstrated more success in China. Areas in which China is actually doing the most innovation (at least on the business model, application, and consumer commercial side) are where the government has a much smaller role.

Huawei benefited from massive state subsidies and theft of intellectual property. But the company has been savvy about how it utilized these advantages: its investments in research and development (R&D) and management strategy contributed to building a powerhouse company that now may be the only company in the world capable of making the full range of 5G products that are widely regarded by U.S. and European carriers to be high quality.

The Honorable Mimi Walters

1. **DHS, as the Sector Specific Agency for Telecom, is looking into both supply chain risks—including 5G and systemic risks more broadly. The FCC's CSRIC is also looking into supply chain risks related to 5G. The FCC CSRIC Report is due in September, and the DHS effort may conclude some time later before the end of the year. How do we avoid duplicative or potentially conflicting recommendations from all of these parallel efforts?**

    a. **Should we vest decision-making at one agency?**

This is a question which falls outside the scope of my expertise.

The Honorable Tim Walberg

1. **When talking about our domestic manufacturing capability, we're also talking about our ability to identify emerging technologies and bring them to commercialization for both U.S. and global markets.**

   My colleagues have expressed the need for a national strategy that addresses threats to our telecommunications networks, to competition in the supply chain, and to national security. Can you elaborate on how human capital – having a technically trained workforce capable of competing on advanced research and development – plays into such a national strategy?

a. **What can Congress do to lead on this piece of the puzzle?**

Congress should work to improve the quality of STEM education as well as expanding access to STEM education and training programs. According to a recent study by CSIS, U.S. government spending levels of education are roughly in line with other advanced economies; however, the United States is declining in math and science test scores. There is also significant disparity between low and high incomes students.

Congress should also work to enable incentives for the top researchers and engineers from around the world to work at U.S. labs and research institutes. Beijing has been attracting top talent from around the world to move to China to lead labs by giving them major sources of funding and other forms of support.

Congress also needs to work to prevent racial and ethnic discrimination against researchers based on country of origin. A recent article in Foreign Policy discusses proposed restrictions on Chinese scientists and researchers in the United States. According to the author, 'The United States may feel it's only playing defense in a global cold war over tech. In reality, these policies play into Beijing's preferred vision of the world. China sees science as a tool of national greatness and scientists as servants to the state. This parochial vision discounts the individual agency and ethical obligations of scientists and runs contrary to the cosmopolitan ideal of science. The United States must uphold those ideals, not create new boundaries.'

<u>The Honorable Anna Eshoo</u>

1. **During my questioning, I asked if anyone had done an analysis on the trusted supply chain to determine whether it is viable for our country to eliminate our dependence on foreign adversarial companies like Huawei and ZTE. You told me it had not, but you would follow up.**

    a. **Have you or anyone begun to conduct such an assessment?**

    b. **If not, are you willing to do so?**

    From a commercial lens, Huawei and ZTE equipment has a reputation for being high quality and affordable. In low income rural areas, there really is no viable alternative. Moreover, as we look to 5G, Huawei is perhaps the one company capable of making products across the 5G stack from handsets to network equipment. Reducing dependence on these vendors is therefore difficult.

2. **Did you agree with the Department of Commerce's decision to implement a seven-year ban on ZTE?**

a. **If so, should the Department and other U.S. officials investigate whether similar bans are appropriate for other Chinese entities, as Senator Rubio has suggested?**

b. Should the Administration continue to indulge ZTE and other companies in 'deals' when we know outright that the company has repeatedly undermined our laws?

ZTE violated U.S. export control law and resisted compliance with investigations. While it is not uncommon for sanctions against companies to be lifted after a period, the timing and process by which the penalties against ZTE were lifted is highly unusual. These factors—speed and the manner by which messaging and negotiating occurred—undermines the credibility of our sanctions system, sending a message to other governments around the world that law enforcement matters are open to political trading. The fate of ZTE has now become intertwined in a complex web involving trade, supply chain cybersecurity, investment, technological competition that is difficult to untangle.

3. What is the potential for harm to our national security by having foreign adversaries involved in business with U.S. small businesses and start-ups?

There is some risk that China would gain market knowledge or technology through investment in early stage U.S. companies, including in areas with dual-use and national security implications. However, this is not necessarily the case, and depends on two main factors: (1) is the Chinese investor just a passive investor or exercising influence in ways that would give then access to the technology; and (2) is the Chinese investor linked to a strategic or military entity through a shell company structure? Increased resources for CFIUS to monitor these factors is a positive development in capturing risk.

But these factors (access to technology and shell company designed to evade scrutiny) should not be assumed in all cases. That is why it is so critical that the decision be made in a precise manner that identifies real threats, but does not sweep up all Chinese investment under a blanket ban.

There are consequences of overreach and using CFIUS as a blunt instrument for U.S. technological leadership and innovation. Passive investments fund U.S. entrepreneurship, human talent, and innovation in emerging technologies, which are needed to stay ahead of China and others. Chinese funds blocked from U.S. markets would instead go to support innovation in other countries, creating a disadvantage for the United States.