Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Ben Sasse (No. 1 to no. 6)
U.S. Senate Committee on the Judiciary
May 14, 2019

Question 1:

Can you clarify the relationship between Huawei, ZTE, and Chinese tech companies and the Chinese Communist Party? How do the interests of one serve the other?

Answer 1:

China is a one party state with no formal checks or balances on its ability to compel citizens or companies to cooperate with its security and intelligence agencies. This is codified in Chinese legislation such as the National Security Law, the National Intelligence Law, the Counter-Terrorism Law, and the Cybersecurity Law. These make clear that if a Chinese company, regardless of whether it is state-owned or private, is directed to collaborate, it has no choice but to do so, and to keep such collaboration secret.

Question 2:

What are the implications for the United States and the global economy if China is able to win the race to 5G dominance?

Answer 2:

China seeks to establish itself as a cyber power and has been rapidly developing a legal framework to enhance its control over data, networks, and information in cyberspace. China's increasing willingness to use all the tools at its disposal poses a significant risk to global communications networks. Allowing telecommunications companies subject to Chinese jurisdiction to dominate international telecommunications networks (including infrastructure such as telephone lines, fiber optic cables, cellular networks, communication satellites, and data centers) would give them greater access to global data and the ability to exploit that access to the detriment of U.S. national security interests. Specifically, such access could be used to skim data and steal intellectual property, as well as to disrupt or turn off global communications networks.

Question 3:

Can you speak a bit more about how our allies and partners in Europe and Asia are thinking about the security implications surrounding 5G? How much do they share our concerns? Why do some of our traditional partners seem to be more accommodating to Huawei technology than we are?

Answer 3:

We have been working with our allies and partners to raise awareness the national security risks associated with using untrusted vendors in 5G networks. Countries around the world are acknowledging that supply chain security is critical to the overall security and reliability of their

future 5G networks. All countries, including our allies and partners, can and should make their own sovereign decisions with a full understanding of the risks and vulnerabilities involved.

Question 4:

How critical is it for our security that our allies have the same view of next generation of technology with a Chinese origin? What are the risks to the United States if they do not share the same view?

Answer 4:

The security of our communications networks is vital not only to U.S. national security, but to the security of our allies and partners. The United States government has been raising awareness among our allies and partners of the national security risks posed by untrusted telecoms equipment vendors like Huawei and ZTE that are subject to unchecked powers of compulsion by an authoritarian government.

Question 5:

What is it going to take for us to have a unified view across our alliances, particularly the NATO alliance?

Answer 5:

The Administration is engaging intensively with international partners, including NATO Allies, on the importance of safeguarding our 5G networks. We stress that the security of our Allies' telecoms networks has a direct bearing on our mutual national security. The presence of untrusted vendors in any of our next-generation wireless networks could impact our ability to share sensitive information and mobilization requirements. Allies have begun to consult on how NATO might approach its future engagement with and related to China. The United States strongly supports NATO doing more to counter potential Chinese threats. The United States also welcomes NATO-EU cooperation on the vulnerabilities posed by the use of Chinese equipment in telecommunications/5G networks. We see this as an area where NATO-EU cooperation would be beneficial given the complex and overlapping concerns between the military and civilian realm, and the overarching security implications for both organizations and for all NATO and EU members.

Question 6:

What is Putin’s view of 5G? How is he working to shape this tech race we are currently engaged in with the China?

Answer 6:

Questions for the Record Submitted to
Deputy Assistant Secretary Robert Strayer by
Senator Ben Sasse (No. 1 to no. 6)
U.S. Senate Committee on the Judiciary
May 14, 2019

In his annual address to the Federal Assembly in February 2019, President Putin identified 5G implementation as a priority for Russia. On June 6, at the Saint Petersburg International Economic Forum, Russia's flagship economic event, Russia's MTS and China's Huawei signed an agreement to build a 5G network in Russia. I am committed to safeguarding our 5G network, and will continue to monitor Russia and China's cooperation in this sphere, and assess how it affects U.S. network security.