III

Calendar No. _____

116TH CONGRESS
1ST SESSION

# S. CON. RES. 10

Recognizing that Chinese telecommunications companies such as Huawei and ZTE pose serious threats to the national security of the United States and its allies.

---

IN THE SENATE OF THE UNITED STATES

MARCH 28, 2019

Mr. GARDNER (for himself, Mr. COONS, Mr. MARKEY, Mr. CRUZ, and Mr. RUBIO) submitted the following concurrent resolution; which was referred to the Committee on Foreign Relations

_____ (legislative day, _____), _____

Reported by Mr. RISCH, with an amendment and an amendment to the preamble

[Strike out all after the resolving clause and insert the part printed in italic]

[Strike the preamble and insert the part printed in italic]

---

# CONCURRENT RESOLUTION

Recognizing that Chinese telecommunications companies such as Huawei and ZTE pose serious threats to the national security of the United States and its allies.

~~Whereas fifth generation (5G) wireless technology promises greater speed and capacity and will provide the backbone for the next generation of digital technologies;~~

~~Whereas fifth generation wireless technology will be a revolutionary advancement in telecommunications with the po-~~

tential to create millions of jobs and billions of dollars in economic opportunity;

Whereas Chinese companies, including Huawei, have invested substantial resources in advancing fifth generation wireless technology and other telecommunications services around the globe, including subsidies provided directly by the Government of the People's Republic of China;

Whereas Chinese officials have increased leadership roles at the International Telecommunications Union, where international telecommunications standards are set, and companies such as Huawei have increased their influence at the 3rd Generation Partnership Project (3GPP), whose work informs global technology standards;

Whereas Huawei and ZTE have aggressively sought to enter into contracts throughout the developing world, including throughout Latin America and Africa in countries such as Venezuela and Kenya;

Whereas, in 2012, the Permanent Select Committee on Intelligence of the House of Representatives released a bipartisan report naming Huawei and ZTE as national security threats;

Whereas, in 2013, the United States restricted Federal procurement of certain products produced by Huawei and ZTE and has since expanded restrictions on Federal procurement of those products;

Whereas, in 2016, the national legislature of the People's Republic of China passed the Cyber Security Law of the People's Republic of China, article 28 of which requires ''network operators'', including companies like Huawei, to ''provide technical support and assistance'' to Chinese authorities involved in national security efforts;

Whereas, in 2017, the national legislature of the People's Republic of China passed the National Intelligence Law of the People's Republic of China, article 7 of which requires "all organizations and citizens"—including companies like Huawei and ZTE—to "support, assist, and cooperate with national intelligence efforts" undertaken by the People's Republic of China;

Whereas, in August 2018, the Government of Australia banned Huawei and ZTE from building the fifth generation wireless networks of Australia;

Whereas, in August 2018, Congress restricted the heads of Federal agencies from procuring certain covered telecommunications equipment and services, which included Huawei and ZTE equipment;

Whereas, in December 2018, the Government of Japan issued instructions effectively banning Huawei and ZTE from official contracts in the country;

Whereas, on December 7, 2018, a Vice-President of the European Commission expressed concern that Huawei and other Chinese companies may be forced to cooperate with China's intelligence services to install "mandatory backdoors" to allow access to encrypted data;

Whereas, in January 2019, the Office of the Director of National Intelligence issued a Worldwide Threat Assessment that describes concerns "about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies";

Whereas, in February 2019, the Government of New Zealand expressed serious concern about Huawei building the fifth generation wireless networks of New Zealand;

~~Whereas the Department of Justice has charged Huawei with the theft of trade secrets, obstruction of justice, and other serious crimes;~~

~~Whereas, against the strong advice of the United States and a number of the security partners of the United States, the governments of countries such as Germany have indicated that they may permit Huawei to build out the fifth generation wireless networks of those countries;~~

~~Whereas installation of Huawei equipment in the communications infrastructure of countries that are allies of the United States would jeopardize the security of communication lines between the United States and those allies;~~

~~Whereas secure communications systems are critical to ensure the safety and defense of the United States and allies of the United States;~~

~~Whereas the North Atlantic Treaty Organization (NATO) and other vital international security arrangements depend on strong and secure communications, which could be put at risk through the use of Huawei and ZTE equipment; and~~

~~Whereas there has been broad bipartisan consensus in Congress for years that Chinese companies like Huawei and ZTE present serious threats to national and global security. Now, therefore, be it~~

*Whereas fifth-generation (in this preamble referred to as "5G") wireless technology promises greater speed and capacity and will provide the backbone for the next generation of digital technologies;*

*Whereas 5G wireless technology will be a revolutionary advancement in telecommunications with the potential to*

*create millions of jobs and billions of dollars in economic opportunity;*

*Whereas Chinese companies, including Huawei, have invested substantial resources in advancing 5G wireless technology and other telecommunications services around the globe, including subsidies provided directly by the Government of the People's Republic of China;*

*Whereas Chinese officials have assumed a greater number of leadership roles at the International Telecommunications Union, where international telecommunications standards are set, and Chinese companies such as Huawei have increased their influence at the 3rd Generation Partnership Project (3GPP), whose work informs global telecommunications network technology standards;*

*Whereas Huawei and ZTE have rapidly expanded their market share throughout the developing world, including in Latin America and Africa, in countries such as Venezuela and Kenya;*

*Whereas, in 2018, Huawei increased its penetration to approximately 29 percent of the global telecommunications equipment market and 43 percent of the market in the Asia-Pacific, according to Dell'Oro Group;*

*Whereas, in 2012, the Permanent Select Committee on Intelligence of the House of Representatives released a bipartisan report naming Huawei and ZTE as national security threats;*

*Whereas, in 2013, the United States restricted Federal procurement of certain products produced by Huawei and ZTE and has since expanded these restrictions;*

*Whereas, in 2016, the national legislature of the People's Republic of China passed the Cyber Security Law of the Peo-*

*ple's Republic of China, Article 28 of which requires "network operators", including companies like Huawei, to "provide technical support and assistance" to Chinese authorities involved in national security efforts;*

*Whereas, in 2017, the national legislature of the People's Republic of China passed the National Intelligence Law of the People's Republic of China, Article 7 of which requires "all organizations and citizens", including companies like Huawei and ZTE, to "support, assist, and cooperate with national intelligence efforts" undertaken by the People's Republic of China;*

*Whereas, in August 2018, the Government of Australia banned Huawei and ZTE from building the 5G wireless networks of Australia;*

*Whereas, in August 2018, Congress restricted the heads of Federal agencies from procuring certain telecommunications equipment and services, which included Huawei and ZTE equipment;*

*Whereas, in December 2018, the Government of Japan issued a directive barring procurement by the government and the Japan Self-Defense Forces of telecommunications equipment that would undermine national security;*

*Whereas, on December 7, 2018, a Vice President of the European Commission expressed concern that Huawei and other Chinese companies may be forced to cooperate with China's intelligence services to install "mandatory backdoors";*

*Whereas, in January 2019, the Office of the Director of National Intelligence issued a Worldwide Threat Assessment that describes concerns "about the potential for Chinese intelligence and security services to use Chinese information*

*technology firms as routine and systemic espionage platforms against the United States and allies";*

*Whereas, in February 2019, the Government of New Zealand expressed serious concern about Huawei building the 5G wireless networks of New Zealand;*

*Whereas, on May 3, 2019, the Prague 5G Security Conference, which was widely attended by representatives from the European Union and the North Atlantic Treaty Organization (NATO), including the United States, produced the Prague Proposals, which state that "communication networks and services should be designed with resilience and security in mind";*

*Whereas the Department of Justice has charged Huawei with the theft of trade secrets, obstruction of justice, and other serious crimes;*

*Whereas, against the strong advice of the United States, the governments of some countries, including United States security partners such as Germany, have indicated they may permit the involvement of Huawei in building 5G wireless networks in those countries;*

*Whereas installation of Huawei equipment in the communications infrastructure of United States allies would jeopardize the security of communication lines between the United States and those allies;*

*Whereas secure communications systems are critical to ensure the safety and defense of the United States and allies of the United States;*

*Whereas the North Atlantic Treaty Organization and other vital international security arrangements, including the Five Eyes partnership, depend on strong and secure com-*

*munications, which could be at risk through the use of Huawei and ZTE equipment; and*

*Whereas there has been broad bipartisan consensus in Congress for years that Chinese companies like Huawei and ZTE present serious threats to national and global security: Now, therefore, be it*

*Resolved by the Senate (the House of Representatives concurring),* ~~That—~~

~~(1) Chinese telecommunications companies such as Huawei and ZTE pose serious threats to the national security of the United States and allies of the United States;~~

~~(2) the United States should reiterate to countries that are choosing to incorporate Huawei or ZTE products in their new telecommunications infrastructure that the United States will consider all necessary measures to limit the risks incurred by entities of the United States Government or Armed Forces from use of such compromised networks;~~

~~(3) the United States should continue to make allies of the United States aware of the ongoing and future risks to telecommunications networks shared between the United States and such allies; and~~

~~(4) the United States should work with the private sector and allies and partners of the United States, including the European Union, in a regular-~~

~~ized bilateral or multilateral format, to identify secure, cost-effective, and reliable alternatives to Huawei or ZTE products.~~

*That—*

*(1) Chinese telecommunications companies such as Huawei and ZTE pose serious threats to the national security of the United States and allies of the United States;*

*(2) the United States should reiterate to countries choosing to incorporate Huawei or ZTE products into their new telecommunications infrastructure that the United States will seek to limit the risks posed to the United States Government or Armed Forces from use of such compromised networks;*

*(3) the United States should continue to make allies of the United States aware of the ongoing and future risks to telecommunications networks shared by the United States and such allies;*

*(4) the United States should work with the private sector and allies and partners, including the European Union, in regularized bilateral or multilateral formats, to identify secure, cost-effective, and reliable alternatives to Huawei or ZTE products; and*

*(5) the United States should accelerate its efforts to increase its leadership and participation in the*

*international fora responsible for global telecommunications standards, and work with allies and partners as well as the private sector to also increase their engagement.*