

Carolina (Ms. MANNING) and the gentlewoman from California (Mrs. KIM).

The Chinese Communist Party does not hide the fact that its end goal is to replace freedom and democracy with dictatorship and oppression, and they use advanced communications such as 5G networks to spread their malign influence. The CCP seeks to spread that influence further by dominating the international standards-setting bodies that set the rules of the road for emerging technologies to skew those standards and industries toward their interests and industries.

This bipartisan bill seeks to bolster U.S. efforts that are already underway, but I think it takes it even further to promote secure telecommunications infrastructure around the world.

It will require, for example, that the U.S. Department of State submit a report on Chinese and Russian efforts to advance their interests at international standards-setting bodies, as my colleague from New Jersey just pointed out, like the International Telecommunication Union, or ITU, and to identify opportunities for multilateral collaboration to promote secure telecom providers.

Lastly, it codifies the International Digital Economy and Telecommunication Advisory Committee, which the State Department created to provide expert advice to the Bureau of Cyberspace and Digital Policy on ICT policy matters.

Mr. Speaker, it is a good bill and deserves the support of Members on both sides. I urge its support, and I yield back the balance of my time.

Mr. MALINOWSKI. Mr. Speaker, I yield 5 minutes to the gentlewoman from North Carolina (Ms. MANNING).

Ms. MANNING. Mr. Speaker, I thank my friend, Representative MALINOWSKI, for yielding. I thank Chairman MEEKS for his leadership in advancing this legislation to the floor, and the gentlewoman from California (Mrs. KIM), my friend, for partnering with me on this important bill.

I rise today in support of my Securing Global Telecommunications Act, a bipartisan bill I introduced to help combat China's attempts to dominate the next generation of critical technology.

Mr. Speaker, many of the products we use every day are connected to telecommunications networks, and they rely on a nearly invisible set of internationally agreed-upon standards.

Our strategic competitors, Russia and China, want to gain an unfair advantage over these critical areas. They are determined to set the rules of the road for the next generation of critical technologies like 5G and AI. They are relentless in their efforts to provide their own companies, like Huawei and ZTE, with an unfair advantage while shutting out all competitors.

This effort is not just about helping their businesses win. This is about controlling a key strategic domain, which poses serious risks and consequences

for the U.S. and global security. That is because the PRC has demonstrated its willingness to abuse technology to steal data, conduct surveillance, and invade privacy, all to further its geopolitical agenda and bolster its model of a closed, authoritarian system of governance.

□ 1515

The United States and our allies must work together to counter this threat. We need to develop and deploy more secure and better trusted tech and telecommunications infrastructure.

My bipartisan bill will help do just that.

First, the bill will require a comprehensive strategy for securing global telecommunications infrastructure worldwide, incorporating mobile networks, data centers, and emerging technologies like LEO satellites and 6G.

We can't afford to be complacent about this challenge. We must have a cohesive strategy to address this issue.

This bill will also help crack down on Russia's and China's malign influence at the International Telecommunication Union, or ITU—a little-known but incredibly important U.N. organization that could determine the standards behind the future of the digital world. It is vital that America and allied countries are in the room at the table and leading the charge to set next-generation technology standards.

Finally, the bill would encourage the U.S. to work closely with our allies and partners to promote and finance secure networks and trusted vendors, without having to rely on Chinese state-owned companies that threaten our security.

Taken together, these important measures will help us shore up key gaps and vulnerabilities, while countering China's strategic technology ambitions.

Mr. Speaker, our adversaries hope and believe that they can achieve undue influence and dominance over international telecom infrastructure and technical standards.

This bill is a step toward stopping their unfettered aggression in an area that is of vital strategic importance.

It will help preserve our global leadership in tech and telecom, keep our companies competitive, and protect the safety and integrity of the networks we rely on every day.

Once again, I thank Chairman MEEKS for his leadership in this area. I urge all my colleagues to join me in supporting this bill.

Mr. MALINOWSKI. Mr. Speaker, H.R. 8503, the Securing Global Telecommunications Act, is important legislation that will position our country to be a leader in the world's telecommunications future. It will ensure that the U.S. Government is taking steps to shore up and protect our digital infrastructure at home and help us better coordinate with like-minded democracies as we work to thwart Russia

and the PRC's malign efforts to crack down on dissent and freedom of expression.

I again thank my colleagues, Representatives MANNING and KIM for introducing this legislation. I hope my colleagues will join me in supporting this bill.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. MALINOWSKI) that the House suspend the rules and pass the bill, H.R. 8503, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. ROSENDALE. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

COUNTERING UNTRUSTED TELECOMMUNICATIONS ABROAD ACT

Mr. MALINOWSKI. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 8520) to establish certain reporting and other requirements relating to telecommunications equipment and services produced or provided by certain entities, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 8520

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Countering Untrusted Telecommunications Abroad Act".

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) the national security of the United States is affected by the telecommunications security of United States allies, partners, and other countries around the globe;

(2) the importance of mobile and internet services makes such services tempting and effective tools for malign influence and economic coercion;

(3) Huawei Technologies Company and ZTE Corporation (and any subsidiary or affiliate of either such entity) should not serve as a vendor of telecommunications equipment or services given the close ties to, and control over, such entities by the People's Republic of China; and

(4) it is in the economic and national security interests of the United States to ensure that countries around the globe use trusted telecommunications equipment or services.

SEC. 3. REPORT ON UNTRUSTED TELECOMMUNICATIONS EQUIPMENT OR SERVICES IN COUNTRIES WITH COLLECTIVE DEFENSE AGREEMENT WITH UNITED STATES.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter for two years, the Secretary of State, in consultation with the Assistant Secretary of Commerce for Communications and Information, shall submit to the Committees on Foreign Affairs and Energy and Commerce of the House of Representatives and the Committees on Foreign

Relations and Commerce, Science, and Transportation of the Senate a report on the prevalence of untrusted telecommunications equipment or services in the networks of United States allies and partners.

(b) MATTERS.—The report under subsection (a) shall enumerate each United States ally or partner with respect to which the United States has entered into a collective defense agreement and include, for each such country, the following:

(1) A description of the presence, or lack thereof, of untrusted telecommunications equipment or services in any 5G network of the country.

(2) If any untrusted telecommunications equipment or service is present in such a network—

(A) an enumeration of any mobile carriers that are using the untrusted telecommunications equipment or service present, and any mobile carriers that are not;

(B) a determination of whether the untrusted telecommunications equipment or service present is in the core or periphery of the network; and

(C) any plans by the United States ally or partner, or the individual mobile carrier, to rip and replace the untrusted telecommunications equipment or service present with a trusted telecommunications equipment or service.

(3) A description of any plans by network operators to use untrusted telecommunications equipment or services in the deployment of Open Radio Access Network (Open RAN) technology, or any successor to such technology, or in future 6G networks.

SEC. 4. REPORT ON COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES IN UNITED STATES EMBASSIES.

(a) FINDINGS.—Congress finds the following:

(1) The Comptroller General of the United States has reported that 23 percent of all telecommunications device manufacturers of the Department of State have at least one supplier reported to be headquartered in the People's Republic of China or the Russian Federation.

(2) The Comptroller General has reported that four percent of all telecommunications contractors of the Department of State have at least one supplier reported to be headquartered in the People's Republic of China.

(b) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State, in consultation with the heads of such other departments and agencies as the Secretary determines necessary, shall submit to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate a report containing an assessment of the use of covered telecommunications equipment or services in United States embassies and by United States embassy staff and personnel.

(2) MATTERS.—The report under paragraph (1) shall include information on the following:

(A) The status of the implementation by the Secretary of State of the prohibition under subsection (a)(1) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232; 132 Stat. 1917; 41 U.S.C. 3901 note prec.) with respect to equipment, systems, and services used at United States embassies, including—

(i) an identification of the United States embassies with respect to which the Secretary has implemented such prohibition, and an identification of those with respect to which the Secretary has not implemented such prohibition, if any;

(ii) an identification of any difficulties that have delayed the implementation of such prohibition by the Secretary with respect to United States embassies, such as visibility into supply chains, costs of equipment replacement, and plans for timely remediation;

(iii) information on any waivers that have been granted to an entity under subsection (d) of such section 889 for equipment, systems, or services used at United States embassies, including a justification of why each waiver was granted and any other information required pursuant to paragraph (1)(B) of such subsection; and

(iv) for any entity that has sought a waiver specified in clause (iii), the implementation status of the phase-out plan of the entity submitted by the entity pursuant to subsection (d) of such section 889.

(B) Information regarding the extent to which the digital devices of United States embassy staff and personnel are serviced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of either such entity), or any other entity headquartered in the People's Republic of China, and an assessment of the likelihood of the intelligence services of the People's Republic of China gaining access to the contents and data of the digital devices used by United States embassy personnel as a result of any such servicing.

(C) Any other information regarding ongoing efforts to safeguard the communications security of United States embassies.

(3) FORM.—The report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

SEC. 5. SUPPORTING TRUSTED TELECOMMUNICATIONS.

(a) IN GENERAL.—The Secretary of State, in consultation with the Assistant Secretary of Commerce for Communications and Information, shall select for the provision of support under this section telecommunications infrastructure projects that have the potential, as determined by the Secretary, to promote the national security of the United States and meet such other requirements as the Secretary may prescribe.

(b) DIPLOMATIC AND POLITICAL SUPPORT.—The Secretary of State shall provide to each project selected under subsection (a), as appropriate, diplomatic and political support, including by using the diplomatic and political influence and expertise of the Department of State to build the capacity of countries to resolve any impediments to the development of the project.

(c) EARLY STAGE PROJECT SUPPORT.—The Director of the United States Trade and Development Agency should provide, as appropriate, early-stage project support with respect to projects selected under subsection (a).

SEC. 6. DISCLOSURE AND TRANSPARENCY OF UNTRUSTED COMMUNICATIONS EQUIPMENT.

(a) IN GENERAL.—Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m) is amended by adding at the end the following new subsection:

“(s) DISCLOSURE OF CERTAIN ACTIVITIES RELATED TO UNTRUSTED TELECOMMUNICATIONS EQUIPMENT.—

“(1) IN GENERAL.—Each issuer required to file an annual or quarterly report under subsection (a) shall disclose in that report the information required in paragraph (2) if, during the period covered by the report, the issuer or any affiliate of the issuer used or contracted to use covered telecommunications equipment or services.

“(2) INFORMATION REQUIRED.—If an issuer or affiliate of the issuer has engaged in an activity described in paragraph (1), the issuer shall disclose such activity, including a detailed description of—

“(A) whether the covered telecommunications equipment or services are being used in a mobile network run by the issuer, and whether those equipment or services were used in the core or periphery of the network;

“(B) whether the covered telecommunications equipment or services were used for cloud computing or data storage;

“(C) whether any covered telecommunications equipment or services were replaced with other vendors; and

“(D) whether the issuer is currently engaging in negotiations or planning to contract to use additional covered telecommunications equipment or services.

“(3) NOTICE OF DISCLOSURES.—If an issuer reports under paragraph (1) that the issuer or an affiliate of the issuer has knowingly engaged in any activity described in that paragraph, the issuer shall separately file with the Commission, concurrently with the annual or quarterly report under subsection (a), a notice that the disclosure of that activity has been included in that annual or quarterly report that identifies the issuer and contains the information required by paragraph (2).

“(4) PUBLIC DISCLOSURE OF INFORMATION.—Upon receiving a notice under paragraph (3) that an annual or quarterly report includes a disclosure of an activity described in paragraph (1), the Commission shall promptly—

“(A) transmit the report to—

“(i) the President;

“(ii) the Committees on Foreign Affairs, Energy and Commerce, and Financial Services of the House of Representatives; and

“(iii) the Committees on Foreign Relations, Commerce, Science, and Transportation, and Banking, Housing, and Urban Affairs of the Senate; and

“(B) make the information provided in the disclosure and the notice available to the public by posting the information on the Internet website of the Commission.

“(5) COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICE DEFINED.—In this subsection, the term ‘covered telecommunications equipment or service’ has the meaning given to the term ‘covered communications equipment or service’ in section 9 of the Secure and Trusted Communications Network Act of 2019 (47 U.S.C. 1608).”

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall take effect with respect to reports required to be filed with the Securities and Exchange Commission after the date that is 180 days after the date of the enactment of this Act.

SEC. 7. DEFINITIONS.

In this Act:

(1) COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICE; UNTRUSTED TELECOMMUNICATIONS EQUIPMENT OR SERVICE.—The terms “covered telecommunications equipment or service” and “untrusted telecommunications equipment or service” have the meaning given to the term “covered communications equipment or service” in section 9 of the Secure and Trusted Communications Network Act of 2019 (47 U.S.C. 1608).

(2) TRUSTED TELECOMMUNICATIONS EQUIPMENT OR SERVICE.—The term “trusted telecommunications equipment or service” means any telecommunications equipment or service that is not a covered telecommunications equipment or service.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. MALINOWSKI) and the gentleman from New Jersey (Mr. SMITH) each will control 20 minutes.

The Chair recognizes the gentleman from New Jersey (Mr. MALINOWSKI).

GENERAL LEAVE

Mr. MALINOWSKI. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 8520.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from New Jersey?

There was no objection.

Mr. MALINOWSKI. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of H.R. 8520, the Countering Untrusted Telecommunications Act.

Imagine the following: A senior official for a NATO ally of the United States transmits a vital national security matter to his country's embassy here in Washington, but before the call even reaches the embassy, it is intercepted by Chinese spyware, which transmits the call to Beijing. Before our officials even hear the top-secret message, CCP officials have captured and recorded the information.

Threats like this are very real and on the rise. Even here in the United States, intelligence and defense officials are concerned that telecommunications equipment made by the company Huawei could capture communications about our nuclear arsenal.

Around the world, the problem is worse. Many of our partners and allies have all of their major cell phone networks backed by unsafe equipment giving the PRC and its friends backdoor access to our private communications. Many countries, replete with this unsafe equipment, have mutual defense treaties with the United States.

The Countering Untrusted Telecommunications Act would be a crucial tool to address these security issues.

First, it would require the State Department to ensure that the Department itself is not relying on unsafe equipment at our embassies around the world.

Second, it would require a comprehensive report on the telecommunications security of all countries with which the United States has a mutual defense treaty.

Third, it authorizes our State Department to provide diplomatic support for telecommunications projects and pushes our United States Trade and Development Agency to finance important projects in this area.

Finally, it requires mobile network operators listed on American stock exchanges to disclose whether they have Huawei, ZTE, or other unsafe equipment in their networks. Currently, many network operators fail to disclose this information despite existing sanctions against Huawei. This provision would be beneficial for our national security but also crucial for investors and shareholders in these companies.

I thank Representatives WILD and WAGNER for their important work on this bill, and I urge all of my colleagues to join me in supporting this legislation.

Mr. Speaker, I reserve the balance of my time.

Mr. SMITH of New Jersey. Mr. Speaker, I rise in support of this bill, and I yield myself such time as I may consume.

Mr. Speaker, the Countering Untrusted Telecommunications Abroad Act requires the State Department to conduct a report on the presence and risks posed by any Chinese telecommunications vendor like Huawei or ZTE in the networks of defense-allied countries.

It also requires the General Accountability Office, or GAO, to report on Chinese and Russian telecom suppliers serving U.S. embassies overseas.

Finally, it tasks the State Department with identifying telecom infrastructure projects that will strengthen U.S. national security, and with helping countries currently being serviced by Chinese vendors to build capacity for replacing those vendors.

I would hope by now that most U.S. officials understand the threats to U.S. national security posed by tech companies controlled by the Chinese Communist Party, like Huawei. But we must also ensure that our allies and partners are not duped by the seemingly low cost of telecom services provided by state-backed countries. While seemingly cheap, the real cost lies in giving the CCP control over all of your telecommunications data, which they will use to spread their malign influence globally.

So I support the bill strongly, and I yield back the balance of my time.

Mr. MALINOWSKI. Mr. Speaker, I am prepared to close, and I yield myself the balance of my time.

Mr. Speaker, H.R. 8520, the Countering Untrusted Telecommunications Act is an important initiative in finding and addressing American vulnerabilities to cyber spying and espionage, particularly in our communications with partners and allies whose unsecure networks may provide backdoor access to these increasing threats.

I, once again, thank Representatives WILD and WAGNER for their tremendous work in advancing this bill and their commitment to protecting our national security from cyber and security threats. I hope my colleagues will join us in supporting this bill.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. MALINOWSKI) that the House suspend the rules and pass the bill, H.R. 8520, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. ROSENDALE. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

RUSSIA CRYPTOCURRENCY
TRANSPARENCY ACT

Mr. MALINOWSKI. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 7338) to require congressional notification prior to payments of Department of State rewards using cryptocurrencies, authorize the appointment of a Director of Digital Currency Security in the Office of Economic Sanctions Policy and Implementation of the Department of State, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 7338

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Russia Cryptocurrency Transparency Act".

SEC. 2. FINDINGS.

Congress finds the following:

(1) On February 24, 2022, the Government of the Russian Federation, led by Vladimir Putin, launched an unprovoked, full-scale invasion of Ukraine.

(2) This unprovoked act of aggression violates Ukraine's right to independence, sovereignty, and territorial integrity, and constitutes an emergency in international relations.

(3) The invasion by the Government of the Russian Federation of Ukraine caused significant displacement in Ukraine and triggered a broader humanitarian crisis in Europe.

(4) On March 23, 2022, the Department of State released a statement assessing that the Russian Armed Forces committed war crimes by launching indiscriminate attacks on civilians and non-military infrastructure, including apartment buildings, schools, and hospitals, leaving thousands of innocent civilians killed or wounded.

(5) The United Nations Office for Coordination of Humanitarian Affairs has projected that, over the next three months, 12,000,000 people living in Ukraine will need humanitarian assistance, 6,700,000 people will be internally displaced, and 4,000,000 people will flee Ukraine.

(6) Rapid humanitarian assistance is necessary across sectors to address the needs of refugees and internally displaced persons from Ukraine.

(7) Cryptocurrency has been used as an effective cross-border payment tool to send millions to the Ukrainian Government, Ukrainian army, and Ukrainian refugees with limited access to financial services.

(8) In response to the war of aggression by the Government of the Russian Federation, the United States has imposed an array of sanctions, cutting off major Russian financial institutions from Western markets and freezing the assets of numerous Russian oligarchs.

(9) Given that regimes sanctioned by the United States have used cryptocurrencies to evade sanctions, there are increasing concerns that these digital assets may be used to circumvent the sanctions now imposed on Russia and Belarus by the United States and other foreign countries.

SEC. 3. CONGRESSIONAL NOTIFICATIONS FOR
STATE DEPARTMENT
CRYPTOCURRENCY REWARDS.

(a) CONGRESSIONAL NOTIFICATION.—Subsection (e) of section 36 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2708) is amended by adding at the end the following new paragraph: