

more important than ever that we continue to stand with the people of Hong Kong.

Mr. Speaker, I want to thank Chairman MEEKS for bringing this resolution which I was proud to join as a lead cosponsor, and I yield back the balance of my time.

□ 1745

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

Mr. Speaker, first, let me thank the ranking member for making sure we make a unified, strong, bipartisan statement, and all of my colleagues on the Foreign Affairs Committee on both sides of the aisle because H. Res. 130 sends a strong and unequivocal message: The United States stands firmly in support of the people of Hong Kong and the rights, freedoms, and autonomy they are promised in the joint declaration and basic law.

This resolution signals that the House's support of the people of Hong Kong and their struggle for democracy shall not waiver and shall remain firm and resolute.

Mr. Speaker, I hope that all of my colleagues will join Ranking Member McCAUL and myself in supporting this resolution, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. MEEKS) that the House suspend the rules and agree to the resolution, H. Res. 130.

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. GOOD of Virginia. Mr. Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

CYBER DIPLOMACY ACT OF 2021

Mr. MEEKS. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 1251) to support United States international cyber diplomacy, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1251

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Cyber Diplomacy Act of 2021”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings.
- Sec. 3. Definitions.
- Sec. 4. United States international cyberspace policy.
- Sec. 5. Department of state responsibilities.
- Sec. 6. International cyberspace executive arrangements.

Sec. 7. International strategy for cyberspace.

Sec. 8. Annual country reports on human rights practices.

Sec. 9. Gao report on cyber diplomacy.

Sec. 10. Sense of congress on cybersecurity sanctions against north korea and cybersecurity legislation in vietnam.

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) The stated goal of the United States International Strategy for Cyberspace, launched on May 16, 2011, is to “work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation . . . in which norms of responsible behavior guide states’ actions, sustain partnerships, and support the rule of law in cyberspace”.

(2) In its June 24, 2013, report, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (referred to in this section as “GGE”), established by the United Nations General Assembly, concluded that “State sovereignty and the international norms and principles that flow from it apply to States’ conduct of [information and communications technology] ICT-related activities and to their jurisdiction over ICT infrastructure with their territory”.

(3) In January 2015, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan proposed a troubling international code of conduct for information security, which could be used as a pretext for restricting political dissent, and includes “curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds”.

(4) In its July 22, 2015, consensus report, GGE found that “norms of responsible State behavior can reduce risks to international peace, security and stability”.

(5) On September 25, 2015, the United States and China announced a commitment that neither country’s government “will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors”.

(6) At the Antalya Summit on November 15 and 16, 2015, the Group of 20 Leaders’ communiqué—

(A) affirmed the applicability of international law to state behavior in cyberspace;

(B) called on states to refrain from cyber-enabled theft of intellectual property for commercial gain; and

(C) endorsed the view that all states should abide by norms of responsible behavior.

(7) The March 2016 Department of State International Cyberspace Policy Strategy noted that “the Department of State anticipates a continued increase and expansion of our cyber-focused diplomatic efforts for the foreseeable future”.

(8) On December 1, 2016, the Commission on Enhancing National Cybersecurity, which was established within the Department of Commerce by Executive Order 13718 (81 Fed. Reg. 7441), recommended that “the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices”.

(9) On April 11, 2017, the 2017 Group of 7 Declaration on Responsible States Behavior in Cyberspace—

(A) recognized “the urgent necessity of increased international cooperation to promote security and stability in cyberspace”;

(B) expressed commitment to “promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States”; and

(C) reaffirmed that “the same rights that people have offline must also be protected online”.

(10) In testimony before the Select Committee on Intelligence of the Senate on May 11, 2017, Director of National Intelligence Daniel R. Coats identified six cyber threat actors, including—

(A) Russia, for “efforts to influence the 2016 U.S. election”;

(B) China, for “actively targeting the U.S. Government, its allies, and U.S. companies for cyber espionage”;

(C) Iran, for “leverag[ing] cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats”;

(D) North Korea, for “previously conduct[ing] cyber-attacks against U.S. commercial entities—specifically, Sony Pictures Entertainment in 2014”;

(E) terrorists, who “use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations”; and

(F) criminals, who “are also developing and using sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activities”.

(11) On May 11, 2017, President Donald J. Trump issued Executive Order 13800 (82 Fed. Reg. 22391), entitled “Strengthening the Cybersecurity of Federal Networks and Infrastructure”, which—

(A) designates the Secretary of State to lead an interagency effort to develop an engagement strategy for international cooperation in cybersecurity; and

(B) notes that “the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining . . . the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft”.

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(2) INFORMATION AND COMMUNICATIONS TECHNOLOGY; ICT.—The terms “information and communications technology” and “ICT” include hardware, software, and other products or services primarily intended to fulfill or enable the function of information processing and communication by electronic means, including transmission and display, including via the Internet.

(3) EXECUTIVE AGENCY.—The term “Executive agency” has the meaning given the term in section 105 of title 5, United States Code.

SEC. 4. UNITED STATES INTERNATIONAL CYBERSPACE POLICY.

(a) IN GENERAL.—It is the policy of the United States to work internationally to

promote an open, interoperable, reliable, unfettered, and secure Internet governed by the multi-stakeholder model, which—

(1) promotes human rights, democracy, and rule of law, including freedom of expression, innovation, communication, and economic prosperity; and

(2) respects privacy and guards against deception, fraud, and theft.

(b) **IMPLEMENTATION.**—In implementing the policy described in subsection (a), the President, in consultation with outside actors, including private sector companies, non-governmental organizations, security researchers, and other relevant stakeholders, in the conduct of bilateral and multilateral relations, shall pursue the following objectives:

(1) Clarifying the applicability of international laws and norms to the use of ICT.

(2) Reducing and limiting the risk of escalation and retaliation in cyberspace, damage to critical infrastructure, and other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public.

(3) Cooperating with like-minded democratic countries that share common values and cyberspace policies with the United States, including respect for human rights, democracy, and the rule of law, to advance such values and policies internationally.

(4) Encouraging the responsible development of new, innovative technologies and ICT products that strengthen a secure Internet architecture that is accessible to all.

(5) Securing and implementing commitments on responsible country behavior in cyberspace based upon accepted norms, including the following:

(A) Countries should not conduct, or knowingly support, cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

(B) Countries should take all appropriate and reasonable efforts to keep their territories clear of intentionally wrongful acts using ICTs in violation of international commitments.

(C) Countries should not conduct or knowingly support ICT activity that, contrary to international law, intentionally damages or otherwise impairs the use and operation of critical infrastructure providing services to the public, and should take appropriate measures to protect their critical infrastructure from ICT threats.

(D) Countries should not conduct or knowingly support malicious international activity that, contrary to international law, harms the information systems of authorized emergency response teams (also known as “computer emergency response teams” or “cybersecurity incident response teams”) of another country or authorize emergency response teams to engage in malicious international activity.

(E) Countries should respond to appropriate requests for assistance to mitigate malicious ICT activity emanating from their territory and aimed at the critical infrastructure of another country.

(F) Countries should not restrict cross-border data flows or require local storage or processing of data.

(G) Countries should protect the exercise of human rights and fundamental freedoms on the Internet and commit to the principle that the human rights that people have offline should also be protected online.

(6) Advancing, encouraging, and supporting the development and adoption of internationally recognized technical standards and best practices.

SEC. 5. DEPARTMENT OF STATE RESPONSIBILITIES.

(a) **IN GENERAL.**—Section 1 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a) is amended—

(1) by redesignating subsection (g) as subsection (h); and

(2) by inserting after subsection (f) the following new subsection:

“(g) **BUREAU OF INTERNATIONAL CYBERSPACE POLICY.**—

“(1) **IN GENERAL.**—There is established, within the Department of State, a Bureau of International Cyberspace Policy (referred to in this subsection as the ‘Bureau’). The head of the Bureau shall have the rank and status of ambassador and shall be appointed by the President, by and with the advice and consent of the Senate.

“(2) **DUTIES.**—

“(A) **IN GENERAL.**—The head of the Bureau shall perform such duties and exercise such powers as the Secretary of State shall prescribe, including implementing the policy of the United States described in section 4 of the Cyber Diplomacy Act of 2021.

“(B) **DUTIES DESCRIBED.**—The principal duties and responsibilities of the head of the Bureau shall be—

“(i) to serve as the principal cyberspace policy official within the senior management of the Department of State and as the advisor to the Secretary of State for cyberspace issues;

“(ii) to lead the Department of State’s diplomatic cyberspace efforts, including efforts relating to international cybersecurity, Internet access, Internet freedom, digital economy, cybercrime, deterrence and international responses to cyber threats, and other issues that the Secretary assigns to the Bureau;

“(iii) to coordinate cyberspace policy and other relevant functions within the Department of State and with other components of the United States Government, including through the Cyberspace Policy Coordinating Committee described in paragraph (6), and by convening other coordinating meetings with appropriate officials from the Department and other components of the United States Government on a regular basis;

“(iv) to promote an open, interoperable, reliable, unfettered, and secure information and communications technology infrastructure globally;

“(v) to represent the Secretary of State in interagency efforts to develop and advance the policy described in section 4 of the Cyber Diplomacy Act of 2021;

“(vi) to act as a liaison to civil society, the private sector, academia, and other public and private entities on relevant international cyberspace issues;

“(vii) to lead United States Government efforts to establish a global deterrence framework for malicious cyber activity;

“(viii) to develop and execute adversary-specific strategies to influence adversary decisionmaking through the imposition of costs and deterrence strategies, in coordination with other relevant Executive agencies;

“(ix) to advise the Secretary and coordinate with foreign governments on external responses to national security-level cyber incidents, including coordination on diplomatic response efforts to support allies threatened by malicious cyber activity, in conjunction with members of the North Atlantic Treaty Organization and other like-minded countries;

“(x) to promote the adoption of national processes and programs that enable threat detection, prevention, and response to malicious cyber activity emanating from the territory of a foreign country, including as such activity relates to the United States’ European allies, as appropriate;

“(xi) to promote the building of foreign capacity relating to cyberspace policy priorities;

“(xii) to promote the maintenance of an open and interoperable Internet governed by the multistakeholder model, instead of by centralized government control;

“(xiii) to promote an international regulatory environment for technology investments and the Internet that benefits United States economic and national security interests;

“(xiv) to promote cross-border flow of data and combat international initiatives seeking to impose unreasonable requirements on United States businesses;

“(xv) to promote international policies to protect the integrity of United States and international telecommunications infrastructure from foreign-based, cyber-enabled threats;

“(xvi) to lead engagement, in coordination with Executive agencies, with foreign governments on relevant international cyberspace and digital economy issues as described in the Cyber Diplomacy Act of 2021;

“(xvii) to promote international policies to secure radio frequency spectrum for United States businesses and national security needs;

“(xviii) to promote and protect the exercise of human rights, including freedom of speech and religion, through the Internet;

“(xix) to promote international initiatives to strengthen civilian and private sector resiliency to threats in cyberspace;

“(xx) to build capacity of United States diplomatic officials to engage on cyberspace issues;

“(xxi) to encourage the development and adoption by foreign countries of internationally recognized standards, policies, and best practices;

“(xxii) to consult, as appropriate, with other Executive agencies with related functions vested in such Executive agencies by law; and

“(xxiii) to conduct such other matters as the Secretary of State may assign.

“(3) **QUALIFICATIONS.**—The head of the Bureau should be an individual of demonstrated competency in the fields of—

“(A) cybersecurity and other relevant cyberspace issues; and

“(B) international diplomacy.

“(4) **ORGANIZATIONAL PLACEMENT.**—During the 1-year period beginning on the date of the enactment of the Cyber Diplomacy Act of 2021, the head of the Bureau shall report to the Under Secretary for Political Affairs or to an official holding a higher position in the Department of State than the Under Secretary for Political Affairs. After the conclusion of such period, the head of the Bureau may report to a different Under Secretary or to an official holding a higher position than Under Secretary if, not less than 15 days prior to any change in such reporting structure, the Secretary of State consults with and provides to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives the following:

“(A) A notification that the Secretary has, with respect to the reporting structure of the Bureau, consulted with and solicited feedback from—

“(i) other relevant Federal entities with a role in international aspects of cyber policy; and

“(ii) the elements of the Department of State with responsibility over aspects of cyber policy, including the elements reporting to—

“(I) the Under Secretary for Political Affairs;

“(II) the Under Secretary for Civilian Security, Democracy, and Human Rights;

“(III) the Under Secretary for Economic Growth, Energy, and the Environment;

“(IV) the Under Secretary for Arms Control and International Security Affairs; and

“(V) the Under Secretary for Management.

“(B) A description of the new reporting structure for the head of the Bureau, as well as a description of the data and evidence used to justify such new structure.

“(C) A plan describing how the new reporting structure will better enable the head of the Bureau to carry out the responsibilities specified in paragraph (2), including the security, economic, and human rights aspects of cyber diplomacy.

“(5) **RULE OF CONSTRUCTION.**—Nothing in this subsection may be construed to preclude the head of the Bureau from being designated as an Assistant Secretary, if such an Assistant Secretary position does not increase the number of Assistant Secretary positions at the Department above the number authorized under subsection (c)(1).

“(6) **COORDINATION.**—

“(A) **CYBERSPACE POLICY COORDINATING COMMITTEE.**—In conjunction with establishing the Bureau pursuant to this subsection, there is established a senior-level Cyberspace Policy Coordinating Committee to ensure that cyberspace issues receive broad senior level-attention and coordination across the Department of State and provide ongoing oversight of such issues. The Cyberspace Policy Coordinating Committee shall be chaired by the head of the Bureau or an official of the Department of State holding a higher position, and operate on an ongoing basis, meeting not less frequently than quarterly. Committee members shall include appropriate officials at the Assistant Secretary level or higher from—

“(i) the Under Secretariat for Political Affairs;

“(ii) the Under Secretariat for Civilian Security, Democracy, and Human Rights;

“(iii) the Under Secretariat for Economic Growth, Energy and the Environment;

“(iv) the Under Secretariat for Arms Control and International Security;

“(v) the Under Secretariat for Management; and

“(vi) other senior level Department participants, as appropriate.

“(B) **OTHER MEETINGS.**—The head of the Bureau shall convene other coordinating meetings with appropriate officials from the Department of State and other components of the United States Government to ensure regular coordination and collaboration on cross-cutting cyber policy issues.

“(b) **SENSE OF CONGRESS.**—It is the sense of Congress that the Bureau of International Cyberspace Policy established under section 1(g) of the State Department Basic Authorities Act of 1956, as added by subsection (a), should have a diverse workforce composed of qualified individuals, including such individuals from traditionally under-represented groups.

“(c) **UNITED NATIONS.**—The Permanent Representative of the United States to the United Nations should use the voice, vote, and influence of the United States to oppose any measure that is inconsistent with the policy described in section 4.”

SEC. 6. INTERNATIONAL CYBERSPACE EXECUTIVE ARRANGEMENTS.

(a) **IN GENERAL.**—The President is encouraged to enter into executive arrangements with foreign governments that support the policy described in section 4.

(b) **TRANSMISSION TO CONGRESS.**—Section 112b of title 1, United States Code, is amended—

(1) in subsection (a) by striking “International Relations” and inserting “Foreign Affairs”;

(2) in subsection (e)(2)(B), by adding at the end the following new clause:

“(iii) A bilateral or multilateral cyberspace agreement.”;

(3) by redesignating subsection (f) as subsection (g); and

(4) by inserting after subsection (e) the following new subsection:

“(f) With respect to any bilateral or multilateral cyberspace agreement under subsection (e)(2)(B)(iii) and the information required to be transmitted to Congress under subsection (a), or with respect to any arrangement that seeks to secure commitments on responsible country behavior in cyberspace consistent with section 4(b)(5) of the Cyber Diplomacy Act of 2021, the Secretary of State shall provide an explanation of such arrangement, including—

“(1) the purpose of such arrangement;

“(2) how such arrangement is consistent with the policy described in section 4 of such Act; and

“(3) how such arrangement will be implemented.”.

(c) **STATUS REPORT.**—During the 5-year period immediately following the transmittal to Congress of an agreement described in clause (iii) of section 112b(e)(2)(B) of title 1, United States Code, as added by subsection (b)(2), or until such agreement has been discontinued, if discontinued within 5 years, the President shall—

(1) notify the appropriate congressional committees if another country fails to adhere to significant commitments contained in such agreement; and

(2) describe the steps that the United States has taken or plans to take to ensure that all such commitments are fulfilled.

(d) **EXISTING EXECUTIVE ARRANGEMENTS.**—Not later than 180 days after the date of the enactment of this Act, the Secretary of State shall brief the appropriate congressional committees regarding any executive bilateral or multilateral cyberspace arrangement in effect before the date of enactment of this Act, including—

(1) the arrangement announced between the United States and Japan on April 25, 2014;

(2) the arrangement announced between the United States and the United Kingdom on January 16, 2015;

(3) the arrangement announced between the United States and China on September 25, 2015;

(4) the arrangement announced between the United States and Korea on October 16, 2015;

(5) the arrangement announced between the United States and Australia on January 19, 2016;

(6) the arrangement announced between the United States and India on June 7, 2016;

(7) the arrangement announced between the United States and Argentina on April 27, 2017;

(8) the arrangement announced between the United States and Kenya on June 22, 2017;

(9) the arrangement announced between the United States and Israel on June 26, 2017;

(10) the arrangement announced between the United States and France on February 9, 2018;

(11) the arrangement announced between the United States and Brazil on May 14, 2018; and

(12) any other similar bilateral or multilateral arrangement announced before such date of enactment.

SEC. 7. INTERNATIONAL STRATEGY FOR CYBERSPACE.

(a) **STRATEGY REQUIRED.**—Not later than one year after the date of the enactment of this Act, the President, acting through the Secretary of State, and in coordination with

the heads of other relevant Federal departments and agencies, shall develop a strategy relating to United States engagement with foreign governments on international norms with respect to responsible state behavior in cyberspace.

(b) **ELEMENTS.**—The strategy required under subsection (a) shall include the following:

(1) A review of actions and activities undertaken to support the policy described in section 4.

(2) A plan of action to guide the diplomacy of the Department of State with regard to foreign countries, including—

(A) conducting bilateral and multilateral activities to—

(i) develop norms of responsible country behavior in cyberspace consistent with the objectives specified in section 4(b)(5); and

(ii) share best practices and advance proposals to strengthen civilian and private sector resiliency to threats and access to opportunities in cyberspace; and

(B) reviewing the status of existing efforts in relevant multilateral fora, as appropriate, to obtain commitments on international norms in cyberspace.

(3) A review of alternative concepts with regard to international norms in cyberspace offered by foreign countries.

(4) A detailed description of new and evolving threats in cyberspace from foreign adversaries, state-sponsored actors, and private actors to—

(A) United States national security;

(B) Federal and private sector cyberspace infrastructure of the United States;

(C) intellectual property in the United States; and

(D) the privacy and security of citizens of the United States.

(5) A review of policy tools available to the President to deter and de-escalate tensions with foreign countries, state-sponsored actors, and private actors regarding threats in cyberspace, the degree to which such tools have been used, and whether such tools have been effective deterrents.

(6) A review of resources required to conduct activities to build responsible norms of international cyber behavior.

(7) A plan of action, developed in consultation with relevant Federal departments and agencies as the President may direct, to guide the diplomacy of the Department of State with regard to inclusion of cyber issues in mutual defense agreements.

(c) **FORM OF STRATEGY.**—

(1) **PUBLIC AVAILABILITY.**—The strategy required under subsection (a) shall be available to the public in unclassified form, including through publication in the Federal Register.

(2) **CLASSIFIED ANNEX.**—The strategy required under subsection (a) may include a classified annex, consistent with United States national security interests, if the Secretary of State determines that such annex is appropriate.

(d) **BRIEFING.**—Not later than 30 days after the completion of the strategy required under subsection (a), the Secretary of State shall brief the appropriate congressional committees on the strategy, including any material contained in a classified annex.

(e) **UPDATES.**—The strategy required under subsection (a) shall be updated—

(1) not later than 90 days after any material change to United States policy described in such strategy; and

(2) not later than one year after the inauguration of each new President.

SEC. 8. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES.

The Foreign Assistance Act of 1961 is amended—

(1) in section 116 (22 U.S.C. 2151n), by adding at the end the following new subsection:

“(h)(1) The report required under subsection (d) shall include an assessment of freedom of expression with respect to electronic information in each foreign country, which information shall include the following:

“(A) An assessment of the extent to which government authorities in the country inappropriately attempt to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion or belief through the Internet, including electronic mail, and a description of the means by which such authorities attempt to inappropriately block or remove such expression.

“(B) An assessment of the extent to which government authorities in the country have persecuted or otherwise punished, arbitrarily and without due process, an individual or group for the nonviolent expression of political, religious, or ideological opinion or belief through the Internet, including electronic mail.

“(C) An assessment of the extent to which government authorities in the country have sought, inappropriately and with malicious intent, to collect, request, obtain, or disclose without due process personally identifiable information of a person in connection with that person’s nonviolent expression of political, religious, or ideological opinion or belief, including expression that would be protected by the International Covenant on Civil and Political Rights, adopted at New York December 16, 1966, and entered into force March 23, 1976, as interpreted by the United States.

“(D) An assessment of the extent to which wire communications and electronic communications are monitored without due process and in contravention to United States policy with respect to the principles of privacy, human rights, democracy, and rule of law.

“(2) In compiling data and making assessments under paragraph (1), United States diplomatic personnel should consult with relevant entities, including human rights organizations, the private sector, the governments of like-minded countries, technology and Internet companies, and other appropriate nongovernmental organizations or entities.

“(3) In this subsection—

“(A) the term ‘electronic communication’ has the meaning given the term in section 2510 of title 18, United States Code;

“(B) the term ‘Internet’ has the meaning given the term in section 231(e)(3) of the Communications Act of 1934 (47 U.S.C. 231(e)(3));

“(C) the term ‘personally identifiable information’ means data in a form that identifies a particular person; and

“(D) the term ‘wire communication’ has the meaning given the term in section 2510 of title 18, United States Code.”; and

(2) in section 502B (22 U.S.C. 2304)—

(A) by redesignating the second subsection (i) (relating to child marriage) as subsection (j); and

(B) by adding at the end the following new subsection:

“(k)(1) The report required under subsection (b) shall include an assessment of freedom of expression with respect to electronic information in each foreign country, which information shall include the following:

“(A) An assessment of the extent to which government authorities in the country inappropriately attempt to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion or belief through the Internet, including electronic mail, and a description of the means by which such authorities attempt to inappropriately block or remove such expression.

“(B) An assessment of the extent to which government authorities in the country have persecuted or otherwise punished, arbitrarily and without due process, an individual or group for the nonviolent expression of political, religious, or ideological opinion or belief through the Internet, including electronic mail.

“(C) An assessment of the extent to which government authorities in the country have sought, inappropriately and with malicious intent, to collect, request, obtain, or disclose without due process personally identifiable information of a person in connection with that person’s nonviolent expression of political, religious, or ideological opinion or belief, including expression that would be protected by the International Covenant on Civil and Political Rights, adopted at New York December 16, 1966, and entered into force March 23, 1976, as interpreted by the United States.

“(D) An assessment of the extent to which wire communications and electronic communications are monitored without due process and in contravention to United States policy with respect to the principles of privacy, human rights, democracy, and rule of law.

“(2) In compiling data and making assessments under paragraph (1), United States diplomatic personnel should consult with relevant entities, including human rights organizations, the private sector, the governments of like-minded countries, technology and Internet companies, and other appropriate nongovernmental organizations or entities.

“(3) In this subsection—

“(A) the term ‘electronic communication’ has the meaning given the term in section 2510 of title 18, United States Code;

“(B) the term ‘Internet’ has the meaning given the term in section 231(e)(3) of the Communications Act of 1934 (47 U.S.C. 231(e)(3));

“(C) the term ‘personally identifiable information’ means data in a form that identifies a particular person; and

“(D) the term ‘wire communication’ has the meaning given the term in section 2510 of title 18, United States Code.”.

SEC. 9. GAO REPORT ON CYBER DIPLOMACY.

Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall submit a report and provide a briefing to the appropriate congressional committees that includes—

(1) an assessment of the extent to which United States diplomatic processes and other efforts with foreign countries, including through multilateral fora, bilateral engagements, and negotiated cyberspace agreements, advance the full range of United States interests in cyberspace, including the policy described in section 4;

(2) an assessment of the Department of State’s organizational structure and approach to managing its diplomatic efforts to advance the full range of United States interests in cyberspace, including a review of—

(A) the establishment of a Bureau in the Department of State to lead the Department’s international cyber mission;

(B) the current or proposed diplomatic mission, structure, staffing, funding, and activities of the Bureau;

(C) how the establishment of the Bureau has impacted or is likely to impact the structure and organization of the Department; and

(D) what challenges, if any, the Department has faced or will face in establishing such Bureau; and

(3) any other matters determined relevant by the Comptroller General.

SEC. 10. SENSE OF CONGRESS ON CYBERSECURITY SANCTIONS AGAINST NORTH KOREA AND CYBERSECURITY LEGISLATION IN VIETNAM.

It is the sense of Congress that—

(1) the President should designate all entities that knowingly engage in significant activities undermining cybersecurity through the use of computer networks or systems against foreign persons, governments, or other entities on behalf of the Government of North Korea, consistent with section 209(b) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9229(b));

(2) the cybersecurity law approved by the National Assembly of Vietnam on June 12, 2018—

(A) may not be consistent with international trade standards; and

(B) may endanger the privacy of citizens of Vietnam; and

(3) the Government of Vietnam should work with the United States and other countries to ensure that such law meets all relevant international standards.

The SPEAKER pro tempore (Ms. GARCIA of Texas). Pursuant to the rule, the gentleman from New York (Mr. MEEKS) and the gentleman from Texas (Mr. MCCAUL) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. MEEKS. Madam Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and to include any extraneous material on H.R. 1251, as amended.

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

There was no objection.

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

Madam Speaker, I rise today in support of H.R. 1251, the Cyber Diplomacy Act of 2021, as amended, by my good friend and the Foreign Affairs Committee’s ranking member, Mr. MCCAUL. I thank him for his work on this important bill.

This Congress, the House Foreign Affairs Committee aims to prioritize efforts to reassert American leadership on a variety of issues. I can’t think of any issue that is more timely than ensuring American leadership is prepared to confront the growing national security challenge in cyberspace.

The U.S. is increasingly under attack online by foreign actors, whether it is the recent SolarWinds hack or other attempted cyber intrusions on critical American infrastructure.

Now more than ever, we need a senior cyber diplomat who can support American efforts to keep the internet open, interoperable, reliable, and secure.

To demonstrate how seriously the United States takes these issues, it is vital that we strengthen the State Department’s tools to address the challenges in cyberspace to American foreign policy. The State Department needs a bureau capable and focused on tackling the growing global challenges of cybersecurity, the digital economy, and internet freedom in order to be

better prepared to advance America's international interests on cyber policy.

Madam Speaker, that is exactly what this Cyber Diplomacy Act will do. Our allies and adversaries are prioritizing international engagement to set the standards and rules that govern how the internet is structured and used. The United States has always been a leader in this space, and now is the time to redouble our efforts to ensure we remain an influential voice in establishing the rules of the road.

It is critical that the United States prioritize our diplomatic efforts in this area and work with our partners and allies to establish agreed-upon norms. To keep the internet open and accessible, we must push back against countries that will exploit the internet to pilfer our intellectual property and hack into our country's most sensitive information, and which seek to derail international norms.

This bill is critical to supporting these key priorities. It authorizes the Bureau of International Cyberspace Policy to lead the State Department's cyber diplomatic efforts, including on issues relating to international cybersecurity, internet access and freedom, and international cyber threats, including countering terrorists' use of cyberspace.

This bill also directs the President to devise a strategy related to U.S. engagement with foreign governments on international norms with respect to responsible state behavior in cyberspace.

I am also pleased that in authorizing this office, we make clear bipartisan congressional intent that the Bureau of International Cyberspace Policy is comprised of a diverse workforce. Like the rest of our national security policy establishments, we know that ensuring a diverse and inclusive workforce improves the effectiveness of national security activities, and this bill makes that intent very clear.

Madam Speaker, I am pleased to support this critical and, again, bipartisan measure that will reassert American leadership on this important issue, and I reserve the balance of my time.

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

Madam Speaker, I am pleased the House is considering the Cyber Diplomacy Act that I reintroduced this Congress with Chairman MEEKS and a strong roster of bipartisan cosponsors. I also want to thank my good friend from Rhode Island (Mr. LANGEVIN), my co-chair on the Congressional Cybersecurity Caucus. Over the past decade, he and I have worked very hard to advance critical cyber legislation like the law that set up the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security.

With today's bill, we are taking the protection provided by CISA to the United States to the international stage and, as the chairman mentioned, providing rules of the road, which we do not have today.

The United States has strategic and economic interests in ensuring the internet remains open, reliable, and secure around the world. Unfortunately, not all governments agree.

For example, Russia and China are aggressively promoting their vision of "cyber sovereignty," which emphasizes state control over cyberspace and tramples individual freedoms. That is why the United States and our allies must be prepared to advance our own vision for cyberspace.

The Cyber Diplomacy Act gives the State Department the necessary tools to work with our allies and partners to stop the spread of misinformation, to stop the cyberattacks, and to stop the imposition of their so-called cyber security.

Madam Speaker, a new ambassador will be given the authority to establish critical cyber norms and standards that do not exist today to help define what is good behavior and what is bad.

Let me say that when the SolarWinds attack occurred, in the past, there were no consequences to bad behavior with the Russians or the Chinese, and I was very supportive and proud that President Biden struck back with sanctions against Russia for this bad behavior. That is what this office is really all about.

Without these clear guidelines, it is not possible to mount a strong response to our adversaries' destructive behavior. This bill is long overdue. To me, it is the last piece in terms of our cyber role in the Federal Government, now taking it to the international stage with our allies around the world.

Madam Speaker, again, I want to thank Chairman MEEKS, Mr. LANGEVIN, and all of the bipartisan cosponsors. The recent high-profile attacks remind us that what happens in cyberspace is vitally important to the United States and our allies and partners around the world. This act will enhance our ability to protect and promote our national security, our ability to compete, and the freedoms and ideals America represents to the world.

A decade ago, we had to determine what is the cyber role—or maybe even 15—what the role is of the Federal Government. We knew the Department of Defense and NSA had great offensive capabilities. We needed a civilian agency to work with the private sector to share threat information, and that became the beginning of the cybersecurity agency at the Department of Homeland Security. And, of course, the FBI investigates. But we have never had any international norms or standards or, as the chairman said, the rules of the road.

This bill, as I said, is long overdue. The Russians influenced our elections. There are, finally, sanctions against them. But before that, few consequences occurred. When the Chinese stole 23 million security clearances, including my own, there was zero response from the United States of America.

When these attacks occurred, and when our intellectual property has been stolen, so much so that Keith Alexander, the NSA Director, said it was the "greatest transfer of wealth in human history," with no consequence, we finally shut down the Chinese consulate in Houston because of the tremendous theft of intellectual property through the Texas Medical Center in my home State, including research and development on the vaccine. Then there was a Texas A&M professor being indicted for espionage for giving NASA data to the Chinese. This has to stop.

This act, this cyber diplomacy bill, will ensure that, at the international level, the United States is respected and that we are going to work with our allies to provide the norms and standards that are so desperately needed to better protect our interests and the interests of our allies.

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

Mr. MEEKS. Madam Speaker, I yield myself the balance of my time.

Madam Speaker, H.R. 1251, the Cyber Diplomacy Act, introduced by my friend and the ranking member, Mr. MCCAUL, is bipartisan legislation that is essential to America's national security and positioning our country to meet the current and future threats in cyberspace head-on.

This bill will give the State Department the tools it needs to further secure peace, stability, and economic prosperity for the United States in the cyber realm now and in the future.

Again, I hope all of my colleagues join both Mr. MCCAUL and myself in supporting this bill, and I yield back the balance of my time.

□ 1800

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. MEEKS) that the House suspend the rules and pass the bill, H.R. 1251, 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. GOOD of Virginia. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

SUPPORTING PEOPLE OF BELARUS AND THEIR DEMOCRATIC ASPIRATIONS AND CONDEMNING ELECTION RIGGING AND SUBSEQUENT VIOLENT CRACKDOWNS ON PEACEFUL PROTESTERS

Mr. MEEKS. Madam Speaker, I move to suspend the rules and agree to the resolution (H. Res. 124) supporting the people of Belarus and their democratic aspirations and condemning the election rigging and subsequent violent