AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—115th Cong., 2d Sess.

H. R. 3776

To support United States international cyber diplomacy, and for other purposes.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Mr. CORKER

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Cyber Diplomacy Act of 2018''.

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

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 6 cyber threat actors, including—

(A) Russia for ''efforts to influence the 2016 US election'';

(B) China, for ''actively targeting the US Government, its allies, and US 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 US commer-

cial 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 fulfil or enable the function of information processing and communication by electronic means, including transmission and display, including via the Internet.

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 multistakeholder 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, nongovernmental 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 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) OFFICE OF CYBERSPACE AND THE DIGITAL ECONOMY.—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:

''(g) OFFICE OF CYBERSPACE AND THE DIGITAL ECONOMY.—

''(1) IN GENERAL.—There is established, within the Department of State, an Office of Cyberspace and the Digital Economy (referred to in this subsection as the 'Office'). The head of the Office 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 Office 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 2018.

"(B) DUTIES DESCRIBED.—The principal duties and responsibilities of the head of the Office shall be—

"(i) to serve as the principal cyber policy official within the senior management of the Department of State and as the advisor to the Secretary of State for cyber 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 Office;

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

"(iv) 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 2018;

"(v) to coordinate cyberspace efforts and other relevant functions, including countering terrorists' use of cyberspace, within the Department of State and with other components of the United States Government;

"(vi) to act as a liaison to public and private sector entities on relevant cyberspace issues;

"(vii) to lead United States Government efforts to establish a global deterrence framework;

"(viii) to develop and execute adversary-specific strategies to influence adversary decisionmaking through the imposition of costs and deterrence strategies;

"(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 to protect the global network with the goal of enabling like-minded participation in deterrence frameworks;

"(xii) to promote the maintenance of an open and interoperable Internet governed by the multi-stakeholder 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 serve as the interagency coordinator for the United States Government on engagement with foreign governments on cyberspace and digital economy issues as described in the Cyber Diplomacy Act of 2018;

"(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 build capacity of United States diplomatic officials to engage on cyber issues;

"(xx) to encourage the development and adoption by foreign countries of inter-

nationally recognized standards, policies, and best practices; and

''(xxi) to promote and advance international policies that protect individuals' private data.

''(3) QUALIFICATIONS.—The head of the Office should be an individual of demonstrated competency in the fields of—

''(A) cybersecurity and other relevant cyber issues; and

''(B) international diplomacy.

''(4) ORGANIZATIONAL PLACEMENT.—During the 4-year period beginning on the date of the enactment of the Cyber Diplomacy Act of 2018, the head of the Office shall report to the Under Secretary for Political Affairs or to an official holding a higher position than the Under Secretary for Political Affairs in the Department of State. After the conclusion of such period, the head of the Office shall report to an appropriate Under Secretary or to an official holding a higher position than Under Secretary.

''(5) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to preclude—

''(A) the Office from being elevated to a Bureau within the Department of State; or

"(B) the head of the Office from being elevated to 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).".

(b) SENSE OF CONGRESS.—It is the sense of Congress that the Office of Cyberspace and the Digital Economy established under section 1(g) of the State Department Basic Authorities Act of 1956, as added by subsection (a), should be a Bureau of the Department of State headed by an Assistant Secretary, subject to the rule of construction specified in paragraph (5)(B) of such section 1(g).

(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:

''(iii) A bilateral or multilateral cyberspace agreement.'';

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

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

''(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 2018, 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 section 112b(e)(2)(B)(iii) 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 meet the 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 1 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 develop norms of responsible country behavior in cyberspace consistent with the objectives under section 4(b)(5); 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—

(A) new and evolving cyberspace threats to United States national security from foreign adversaries, state-sponsored actors, and private actors;

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

(C) intellectual property in the United States; and

(D) the privacy 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 1 year after the inauguration of each new President.

(f) PREEXISTING REQUIREMENT.—The Recommendations to the President on Protecting American Cyber Interests through International Engagement, prepared by the Office of the Coordinator for Cyber Issues

on May 31, 2018, pursuant to section 3(c) of Executive Order 13800 (82 Fed. Reg. 22391), shall be deemed to satisfy the requirement under subsection (a).

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

Section 116 of the Foreign Assistance Act of 1961 (22 U.S.C. 2151n) is amended by adding at the end the following:

''(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 that includes 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 compa-

nies, 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 THREATS AND DATA MISUSE.

Not later than 1 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) a description of the primary threats to the personal information of United States citizens from international actors within the cyberspace domain;

(2) 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, strengthen the protections of United States citizens' personal information;

(3) an assessment of the Department of State's report in response to Executive Order 13800 (82 Fed. Reg. 22391), which documents an engagement strategy for international cooperation in cybersecurity and the extent to which this strategy addresses protections of United States citizens' personal information;

(4) recommendations for United States policymakers on methods to properly address and strengthen the protections of United States citizens' personal information from misuse by international actors; and

(5) any other matters deemed 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 legislation 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—

(A) delay the implementation of the legislation referred to in paragraph (2); and

(B) work with the United States and other countries to ensure that such law meets all relevant international standards.