115TH CONGRESS
2D SESSION

H. R. 3776

IN THE SENATE OF THE UNITED STATES

JANUARY 18, 2018

Received; read twice and referred to the Committee on Foreign Relations

AN ACT

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

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 ''Cyber Diplomacy Act of 2017''.

SEC. 2. FINDINGS.

Congress finds the following:

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

(3) On January 13, 2015, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan proposed a troubling international code of conduct for information security which defines responsible State behavior in cyberspace to include ''curbing the dissemination of information'' and the ''right to independent control of information and communications technology'' when a country's political security is threatened.

(4) The July 22, 2015, GGE consensus report 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 from November 15–16, 2015, the Group of 20 (G20) Leaders' Communique affirmed the applicability of international law to State behavior in cyberspace, called on States to refrain from cyber-enabled theft of intellectual prop-

erty for commercial gain, and 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 established within the Department of Commerce recommended ''the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices.''.

(9) The 2017 Group of 7 (G7) Declaration on Responsible States Behavior in Cyberspace recognized on April 11, 2017, ''the urgent necessity of increased international cooperation to promote security and stability in cyberspace * * * consisting 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 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, the Director of National Intelligence identified six cyber threat actors, including Russia for ''efforts to influence the 2016 US election''; China, for ''actively targeting the US Government, its allies, and US companies for cyber espionage''; Iran for ''leverage[ing] cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats''; North Korea for ''previously conduct[ing] cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014''; terrorists, who ''use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations''; and 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 Trump issued Presidential Executive Order No. 13800 on Strengthening the Cybersecurity of Federal Networks and Infrastructure which designated the Sec-

retary of State to lead an interagency effort to develop strategic options for the President to deter adversaries from cyber threats and an engagement strategy for international cooperation in cybersecurity, noting 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 deception, fraud, and theft.''.

SEC. 3. UNITED STATES INTERNATIONAL CYBERSPACE POLICY.

(a) IN GENERAL.—Congress declares that it is the policy of the United States to work internationally with allies and other partners to promote an open, interoperable, reliable, unfettered, and secure internet governed by the multistakeholder model which promotes human rights, democracy, and rule of law, including freedom of expression, innovation, communication, and economic prosperity, while respecting privacy and guarding against deception, fraud, and theft.

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

(1) Clarifying the applicability of international laws and norms, including the law of armed conflict, to the use of ICT.

(2) Clarifying that countries that fall victim to malicious cyber activities have the right to take proportionate countermeasures under international law, provided such measures do not violate a fundamental human right or peremptory norm.

(3) Reducing and limiting the risk of escalation and retaliation in cyberspace, such as massive denial-of-service attacks, damage to critical infrastructure, or other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public.

(4) 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.

(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 cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

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

(D) 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, and should take appropriate measures to protect their critical infrastructure from ICT threats.

(E) Countries should not conduct or knowingly support malicious international activity that, contrary to international law, harms the information systems of authorized emergency response teams (sometimes known as ''computer emergency response teams'' or ''cybersecurity incident response teams'') or related private sector companies of another country.

(F) Countries should identify economic drivers and incentives to promote securely-designed ICT products and to develop policy and legal frameworks to promote the development of secure internet architecture.

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

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

(I) 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 enjoy the same protections online.

SEC. 4. DEPARTMENT OF STATE RESPONSIBILITIES.

(a) OFFICE OF CYBER ISSUES.—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) OFFICE OF CYBER ISSUES.—

''(1) IN GENERAL.—There is established an Office of Cyber Issues (in this subsection referred to as the 'Office'). The head of the Office shall have the rank and status of ambassador and 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 3 of the Cyber Diplomacy Act of 2017.

''(B) DUTIES DESCRIBED.—The principal duties of the head of the Office shall be to—

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

''(ii) lead the Department of State's diplomatic cyberspace efforts generally, including relating to international cybersecurity, internet access, internet freedom, digital economy, cybercrime, deterrence and international responses to cyber threats;

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

''(iv) represent the Secretary of State in interagency efforts to develop and advance the United States international cyberspace policy;

''(v) coordinate within the Department of State and with other components of the United States Government cyber-

space efforts and other relevant functions, including countering terrorists' use of cyberspace; and

''(vi) act as liaison to public and private sector entities on relevant cyberspace issues.

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

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

''(B) international diplomacy.

''(4) ORGANIZATIONAL PLACEMENT.—The head of the Office shall report to the Under Secretary for Political Affairs or official holding a higher position in the Department of State.

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

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

''(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 Cyber Issues established under section 1(g) of the State Department Basic Authorities Act of 1956 (as amended by subsection (a) of this section) 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 shall use the voice, vote, and influence of the United States to oppose any measure that is inconsistent with the United States international cyberspace policy described in section 3.

SEC. 5. INTERNATIONAL CYBERSPACE EXECUTIVE ARRANGEMENTS.

(a) IN GENERAL.—The President is encouraged to enter into executive arrangements with foreign governments that support the United States international cyberspace policy described in section 3.

(b) TRANSMISSION TO CONGRESS.—The text of any executive arrangement (including the text of any oral arrangement, which shall be reduced to writing) entered into by the United States under subsection (a) shall be trans-

mitted to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate not later than 5 days after such arrangement is signed or otherwise agreed to, together with an explanation of such arrangement, its purpose, how such arrangement is consistent with the United States international cyberspace policy described in section 3, and how such arrangement will be implemented.

(c) STATUS REPORT.—Not later than 1 year after the text of an executive arrangement is transmitted to Congress pursuant to subsection (b) and annually thereafter for 7 years, or until such an arrangement has been discontinued, the President shall report to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate on the status of such arrangement, including an evidence-based assessment of whether all parties to such arrangement have fulfilled their commitments under such arrangement and if not, what steps the United States has taken or plans to take to ensure all such commitments are fulfilled, whether the stated purpose of such arrangement is being achieved, and whether such arrangement positively impacts building of cyber norms internationally. Each such report shall include metrics to support its findings.

(d) EXISTING EXECUTIVE ARRANGEMENTS.—Not later than 60 days after the date of the enactment of this Act, the President shall satisfy the requirements of subsection (c) for the following executive arrangements already in effect:

(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) Any other similar bilateral or multilateral arrangement announced before the date of the enactment of this Act.

SEC. 6. INTERNATIONAL STRATEGY FOR CYBERSPACE.

(a) STRATEGY REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Secretary of State, in coordination with the heads of other relevant Federal departments and agencies, shall produce a strategy relating to United States international policy with regard to cyberspace.

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

(1) A review of actions and activities undertaken to support the United States international cyberspace policy described in section 3.

(2) A plan of action to guide the diplomacy of the Department of State with regard to foreign countries, including conducting bilateral and multilateral activities to develop the norms of responsible international behavior in cyberspace, and status review of existing efforts in multilateral fora to obtain agreements 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 to United States national security in cyberspace from foreign countries, State-sponsored actors, and private actors to Federal and private sector infrastructure of the United States, intellectual property in the United States, and 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, and to what degree such tools have been used and whether or not such tools have been effective.

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

(7) A clarification of the applicability of international laws and norms, including the law of armed conflict, to the use of ICT.

(8) A clarification that countries that fall victim to malicious cyber activities have the right to take proportionate countermeasures under international law, including exercising the right to collective and individual self-defense.

(9) A plan of action to guide the diplomacy of the Department of State with regard to existing mutual defense agreements, including the inclusion in such agreements of information relating to the applicability of malicious cyber activities in triggering mutual defense obligations.

(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.—

(A) IN GENERAL.—If the Secretary of State determines that such is appropriate, the strategy required under subsection (a) may include a classified annex consistent with United States national security interests.

(B) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed as authorizing the public disclosure of an unclassified annex under subparagraph (A).

(d) BRIEFING.—Not later than 30 days after the production of the strategy required under subsection (a), the Secretary of State shall brief the Committee on Foreign Affairs of the House of Representatives and the Com-

mittee on Foreign Relations of the Senate on such 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 there has been any material change to United States policy as described in such strategy; and

(2) not later than 1 year after each inauguration of a new President.

(f) PREEXISTING REQUIREMENT.—Upon the production and publication of the report required under section 3(c) of the Presidential Executive Order No. 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure on May 11, 2017, such report shall be considered as satisfying the requirement under subsection (a) of this section.

SEC. 7. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES.

(a) REPORT RELATING TO ECONOMIC ASSISTANCE.—Section 116 of the Foreign Assistance Act of 1961 (22 U.S.C. 2151n) is amended by adding at the end the following new subsection:

''(h)(1) The report required by subsection (d) shall include an assessment of freedom of expression with re-

spect to electronic information in each foreign country. Such assessment shall consist of the following:

''(A) An assessment of the extent to which government authorities in each country inappropriately attempt to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion or belief via the internet, including electronic mail, as well as a description of the means by which such authorities attempt to block or remove such expression.

''(B) An assessment of the extent to which government authorities in each country have persecuted or otherwise punished an individual or group for the nonviolent expression of political, religious, or ideological opinion or belief via the internet, including electronic mail.

''(C) An assessment of the extent to which government authorities in each country have sought to inappropriately collect, request, obtain, or disclose personally identifiable information of a person in connection with such 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.

''(D) An assessment of the extent to which wire communications and electronic communications are monitored without regard to the principles of privacy, human rights, democracy, and rule of law.

''(2) In compiling data and making assessments for the purposes of paragraph (1), United States diplomatic personnel shall consult with human rights organizations, technology and internet companies, and other appropriate nongovernmental organizations.

''(3) In this subsection—

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

''(B) the term 'internet' has the meaning given such 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 such term in section 2510 of title 18, United States Code.''.

(b) REPORT RELATING TO SECURITY ASSISTANCE.—Section 502B of the Foreign Assistance Act of 1961 (22 U.S.C. 2304) is amended—

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

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

''(k)(1) The report required by subsection (b) shall include an assessment of freedom of expression with respect to electronic information in each foreign country. Such assessment shall consist of the following:

''(A) An assessment of the extent to which government authorities in each country inappropriately attempt to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion or belief via the internet, including electronic mail, as well as a description of the means by which such authorities attempt to block or remove such expression.

''(B) An assessment of the extent to which government authorities in each country have persecuted or otherwise punished an individual or group for the nonviolent expression of political, religious, or ideological opinion or belief via the internet, including electronic mail.

''(C) An assessment of the extent to which government authorities in each country have sought to

inappropriately collect, request, obtain, or disclose personally identifiable information of a person in connection with such 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.

''(D) An assessment of the extent to which wire communications and electronic communications are monitored without regard to the principles of privacy, human rights, democracy, and rule of law.

''(2) In compiling data and making assessments for the purposes of paragraph (1), United States diplomatic personnel shall consult with human rights organizations, technology and internet companies, and other appropriate nongovernmental organizations.

''(3) In this subsection—

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

''(B) the term 'internet' has the meaning given such 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 such term in section 2510 of title 18, United States Code.''.

Passed the House of Representatives January 17, 2018.

Attest: KAREN L. HAAS,

Clerk.