

.....  
(Original Signature of Member)

115TH CONGRESS  
1ST SESSION

**H. R.** \_\_\_\_\_

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

\_\_\_\_\_  
IN THE HOUSE OF REPRESENTATIVES

Mr. ROYCE of California introduced the following bill; which was referred to the Committee on \_\_\_\_\_

\_\_\_\_\_  
**A BILL**

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

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cyber Diplomacy Act  
5 of 2017”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

8 (1) The stated goal of the United States’ Inter-  
9 national Strategy for Cyberspace, launched on May

1       16, 2011, is to “work internationally to promote an  
2       open, interoperable, secure, and reliable information  
3       and communications infrastructure that supports  
4       international trade and commerce, strengthens inter-  
5       national security, and fosters free expression and in-  
6       novation. . . in which norms of responsible behavior  
7       guide states’ actions, sustain partnerships, and sup-  
8       port the rule of law in cyberspace.”.

9               (2) The Group of Governmental Experts (GGE)  
10       on Developments in the Field of Information and  
11       Telecommunications in the Context of International  
12       Security, established by the United Nations General  
13       Assembly, concluded in its June 24, 2013, report  
14       “that State sovereignty and the international norms  
15       and principles that flow from it apply to States’ con-  
16       duct of [information and communications technology  
17       or ICT] related activities and to their jurisdiction  
18       over ICT infrastructure with their territory.”.

19               (3) On January 13, 2015, China, Kazakhstan,  
20       Kyrgyzstan, Russia, Tajikistan, and Uzbekistan pro-  
21       posed a troubling international code of conduct for  
22       information security which defines responsible state  
23       behavior in cyberspace to include “curbing the dis-  
24       semination of information” and the “right to inde-  
25       pendent control of information and communications

1       technology” when a country’s political security is  
2       threatened.

3           (4) The July 22, 2015, GGE consensus report  
4       found that, “norms of responsible State behavior can  
5       reduce risks to international peace, security and sta-  
6       bility.”.

7           (5) On September 25, 2015, the United States  
8       and China announced a commitment “that neither  
9       country’s government will conduct or knowingly sup-  
10      port cyber-enabled theft of intellectual property, in-  
11      cluding trade secrets or other confidential business  
12      information, with the intent of providing competitive  
13      advantages to companies or commercial sectors.”.

14          (6) At the Antalya Summit from November 15-  
15      16, 2015, the Group of 20 (G20) Leaders’ Commu-  
16      nique affirmed the applicability of international law  
17      to state behavior in cyberspace, called on states to  
18      refrain from cyber-enabled theft of intellectual prop-  
19      erty for commercial gain, and endorsed the view that  
20      all states should abide by norms of responsible be-  
21      havior.

22          (7) The March 2016 Department of State  
23      International Cyberspace Policy Strategy noted that,  
24      “the Department of State anticipates a continued in-

1       crease and expansion of our cyber-focused diplomatic  
2       efforts for the foreseeable future.”.

3           (8) On December 1, 2016, the Commission on  
4       Enhancing National Cybersecurity established within  
5       the Department of Commerce recommended “the  
6       President should appoint an Ambassador for Cyber-  
7       security to lead U.S. engagement with the inter-  
8       national community on cybersecurity strategies,  
9       standards, and practices.”.

10          (9) The 2017 Group of 7 (G7) Declaration on  
11       Responsible States Behavior in Cyberspace recog-  
12       nized on April 11, 2017, “the urgent necessity of in-  
13       creased international cooperation to promote secu-  
14       rity and stability in cyberspace. . . consisting of the  
15       applicability of existing international law to State  
16       behavior in cyberspace, the promotion of voluntary,  
17       non-binding norms of responsible State behavior  
18       during peacetime” and reaffirmed “that the same  
19       rights that people have offline must also be pro-  
20       tected online.”.

21          (10) In testimony before the Select Committee  
22       on Intelligence of the Senate on May 11, 2017, the  
23       Director of National Intelligence identified six cyber  
24       threat actors, including Russia for “efforts to influ-  
25       ence the 2016 US election”; China, for “actively tar-

1        getting the US Government, its allies, and US com-  
2        panies for cyber espionage”; Iran for “leverage[ing]  
3        cyber espionage, propaganda, and attacks to support  
4        its security priorities, influence events and foreign  
5        perceptions, and counter threats”; North Korea for  
6        “previously conduct[ing] cyber-attacks against US  
7        commercial entities—specifically, Sony Pictures En-  
8        tertainment in 2014”; terrorists, who “use the Inter-  
9        net to organize, recruit, spread propaganda, raise  
10       funds, collect intelligence, inspire action by followers,  
11       and coordinate operations”; and criminals who “are  
12       also developing and using sophisticated cyber tools  
13       for a variety of purposes including theft, extortion,  
14       and facilitation of other criminal activities”.

15            (11) On May 11, 2017, President Trump issued  
16       Presidential Executive Order 13800 on Strength-  
17       ening the Cybersecurity of Federal Networks and In-  
18       frastructure which designated the Secretary of State  
19       to develop an engagement strategy for international  
20       cooperation in cybersecurity, and noted that “the  
21       United States is especially dependent on a globally  
22       secure and resilient internet and must work with al-  
23       lies and other partners” toward maintaining “the  
24       policy of the executive branch to promote an open,  
25       interoperable, reliable, and secure internet that fos-

1       ters efficiency, innovation, communication, and eco-  
2       nomic prosperity, while respecting privacy and  
3       guarding against deception, fraud, and theft.”.

4       **SEC. 3. UNITED STATES INTERNATIONAL CYBERSPACE**  
5                                   **POLICY.**

6       (a) IN GENERAL.—Congress declares that it is the  
7       policy of the United States to work internationally with  
8       allies and other partners to promote an open, interoper-  
9       able, reliable, unfettered, and secure internet governed by  
10      the multistakeholder model which promotes human rights,  
11      democracy, and rule of law, including freedom of expres-  
12      sion, innovation, communication, and economic prosperity,  
13      while respecting privacy and guarding against deception,  
14      fraud, and theft.

15      (b) IMPLEMENTATION.—In implementing the policy  
16      described in subsection (a), the President, in consultation  
17      with outside actors, including technology companies, non-  
18      governmental organizations, and security researchers,  
19      shall pursue the following objectives in the conduct of bi-  
20      lateral and multilateral relations:

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

24                   (2) Clarifying that countries that fall victim to  
25                   malicious cyber activities have the right to take pro-

1       portionate countermeasures under international law,  
2       provided such measures do not violate a funda-  
3       mental human right or peremptory norm.

4           (3) Reducing and limiting the risk of escalation  
5       and retaliation in cyberspace, such as massive de-  
6       nial-of-service attacks, damage to critical infrastruc-  
7       ture, or other malicious cyber activity that impairs  
8       the use and operation of critical infrastructure that  
9       provides services to the public.

10          (4) Cooperating with like-minded democratic  
11       countries that share common values and cyberspace  
12       policies with the United States, including respect for  
13       human rights, democracy, and rule of law, to ad-  
14       vance such values and policies internationally.

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

18           (A) Countries should not conduct or know-  
19       ingly support cyber-enabled theft of intellectual  
20       property, including trade secrets or other con-  
21       fidential business information, with the intent  
22       of providing competitive advantages to compa-  
23       nies or commercial sectors.

24           (B) Countries should cooperate in devel-  
25       oping and applying measures to increase sta-

1           bility and security in the use of ICTs and to  
2           prevent ICT practices that are acknowledged to  
3           be harmful or that may pose threats to inter-  
4           national peace and security.

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

9           (D) Countries should not conduct or know-  
10          ingly support ICT activity that, contrary to  
11          international law, intentionally damages or oth-  
12          erwise impairs the use and operation of critical  
13          infrastructure, and should take appropriate  
14          measures to protect their critical infrastructure  
15          from ICT threats.

16          (E) Countries should not conduct or know-  
17          ingly support malicious international activity  
18          that, contrary to international law, harms the  
19          information systems of authorized emergency  
20          response teams (sometimes known as “com-  
21          puter emergency response teams” or “cyberse-  
22          curity incident response teams”) or related pri-  
23          vate sector companies of another country.

24          (F) Countries should identify economic  
25          drivers and incentives to promote securely-de-



1 signed ICT products and to develop policy and  
2 legal frameworks to promote the development of  
3 secure internet architecture.

4 (G) Countries should respond to appro-  
5 priate requests for assistance to mitigate mali-  
6 cious ICT activity aimed at the critical infra-  
7 structure of another country emanating from  
8 their territory.

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

12 (I) Countries should protect the exercise of  
13 human rights and fundamental freedoms on the  
14 Internet and commit to the principle that the  
15 human rights that people have offline enjoy the  
16 same protections online.

17 **SEC. 4. DEPARTMENT OF STATE RESPONSIBILITIES.**

18 (a) OFFICE OF CYBER ISSUES.—Section 1 of the  
19 State Department Basic Authorities Act of 1956 (22  
20 U.S.C. 2651a) is amended—

21 (1) by redesignating subsection (g) as sub-  
22 section (h); and

23 (2) by inserting after subsection (f) the fol-  
24 lowing new subsection:

25 “(g) OFFICE OF CYBER ISSUES.—

1           “(1) IN GENERAL.—There is established an Of-  
2           fice of Cyber Issues (in this subsection referred to  
3           as the ‘Office’). The head of the Office shall have  
4           the rank and status of ambassador and be appointed  
5           by the President, by and with the advice and consent  
6           of the Senate.

7           “(2) DUTIES.—

8           “(A) IN GENERAL.—The head of the Of-  
9           fice shall perform such duties and exercise such  
10          powers as the Secretary of State shall prescribe,  
11          including implementing the policy of the United  
12          States described in section 3 of the Cyber Di-  
13          plomacy Act of 2017.

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

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

20                 “(ii) lead the Department of State’s  
21                 diplomatic cyberspace efforts generally, in-  
22                 cluding relating to international cybersecu-  
23                 rity, internet access, internet freedom, dig-  
24                 ital economy, cybercrime, deterrence and  
25                 international responses to cyber threats;

1 “(iii) promote an open, interoperable,  
2 reliable, unfettered, and secure information  
3 and communications technology infrastruc-  
4 ture globally;

5 “(iv) represent the Secretary of State  
6 in interagency efforts to develop and ad-  
7 vance the United States international  
8 cyberspace policy;

9 “(v) coordinate cyberspace efforts and  
10 other relevant functions within the Depart-  
11 ment of State, and with other components  
12 of the United States Government, includ-  
13 ing—

14 “(I) the Department of Com-  
15 merce

16 “(II) the Department of Defense;

17 “(III) the Department of Energy;

18 “(IV) the Department of Home-  
19 land Security;

20 “(V) the Department of Justice;

21 “(VI) Department of the Treas-  
22 ury;

23 “(VII) the Intelligence Commu-  
24 nity; and

1                   “(VIII) the National Security  
2                   Council; and

3                   “(vi) act as liaison to public and pri-  
4                   vate sector entities on relevant cyberspace  
5                   issues.

6                   “(3) QUALIFICATIONS.—The head of the Office  
7                   should be an individual of demonstrated competency  
8                   in the field of—

9                   “(A) cybersecurity and other relevant cyber  
10                  issues; and

11                  “(B) international diplomacy.

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

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

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

20                  “(B) the head of the Office from being ele-  
21                  vated to an Assistant Secretary, if such an As-  
22                  sistant Secretary position does not increase the  
23                  number of Assistant Secretary positions at the  
24                  Department above the number authorized under  
25                  subsection (c)(1).”.

1 (b) UNITED NATIONS.—The Permanent Representa-  
2 tive of the United States to the United Nations shall use  
3 the voice, vote, and influence of the United States to op-  
4 pose any measure that is inconsistent with the United  
5 States international cyberspace policy described in section  
6 3.

7 **SEC. 5. INTERNATIONAL CYBERSPACE EXECUTIVE**  
8 **ARRANGEMENTS.**

9 (a) IN GENERAL.—The President is encouraged to  
10 enter into executive arrangements with foreign govern-  
11 ments that support the United States international cyber-  
12 space policy described in section 3.

13 (b) SUBMISSION TO CONGRESS.—The formal or in-  
14 formal text of any executive arrangement entered into by  
15 the United States under subsection (a) shall be trans-  
16 mitted to the Committee on Foreign Affairs of the House  
17 of Representatives and the Committee on Foreign Rela-  
18 tions of the Senate not later than five days after such ar-  
19 rangement is signed or otherwise agreed to, together with  
20 an explanation of such arrangement, its purpose, how such  
21 arrangement is consistent with the United States inter-  
22 national cyberspace policy described in section 3, and how  
23 such arrangement will be implemented.

24 (c) STATUS REPORT.—Not later than one year after  
25 the formal or informal text of an executive arrangement

1 is submitted to Congress pursuant to subsection (b) and  
2 annually thereafter for seven years, or until such an ar-  
3 rangement has been discontinued, the Secretary of State  
4 shall report to the Committee on Foreign Affairs of the  
5 House of Representatives and the Committee on Foreign  
6 Relations of the Senate on the status of such arrangement,  
7 including an evidence-based assessment of whether all par-  
8 ties to such arrangement have fulfilled their commitments  
9 under such arrangement, whether the stated purpose of  
10 such arrangement is being achieved, and whether such ar-  
11 rangement positively impacts building of cyber norms  
12 internationally. Each such report shall include metrics to  
13 support its findings.

14 (d) EXISTING EXECUTIVE ARRANGEMENTS.—Not  
15 later than 60 days after the date of the enactment of this  
16 Act, the President shall satisfy the requirements of sub-  
17 section (c) for the following executive arrangements al-  
18 ready in effect:

19 (1) The arrangement announced between the  
20 United States and Japan on April 25, 2014.

21 (2) The arrangement announced between the  
22 United States and the United Kingdom on January  
23 16, 2015.

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

1           (4) The arrangement announced between the  
2 United States and Korea on October 16, 2015.

3           (5) The arrangement announced between the  
4 United States and Australia on January 19, 2016.

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

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

9           (8) The arrangement announced between the  
10 United States and Kenya on June 22, 2017.

11           (9) The arrangement announced between the  
12 United States and Israel on June 26, 2017.

13           (10) Any other similar bilateral or multilateral  
14 arrangement announced before the date of the en-  
15 actment of this Act.

16 **SEC. 6. INTERNATIONAL STRATEGY FOR CYBERSPACE.**

17           (a) **STRATEGY REQUIRED.**—Not later than one year  
18 after the date of the enactment of this Act, the Secretary  
19 of State, in coordination with the heads of other relevant  
20 Federal departments and agencies, shall produce a strat-  
21 egy relating to United States international policy with re-  
22 gard to cyberspace.

23           (b) **ELEMENTS.**—The strategy required under sub-  
24 section (a) shall include the following:

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

4           (2) A plan of action to guide the diplomacy of  
5 the Department of State with regard to foreign  
6 countries, including conducting bilateral and multi-  
7 lateral activities to develop the norms of responsible  
8 international behavior in cyberspace, and status re-  
9 view of existing efforts in multilateral fora to obtain  
10 agreements on international norms in cyberspace.

11          (3) A review of alternative concepts with regard  
12 to international norms in cyberspace offered by for-  
13 eign countries.

14          (4) A detailed description of new and evolving  
15 threats to United States national security in cyber-  
16 space from foreign countries, state-sponsored actors,  
17 and private actors to Federal and private sector in-  
18 frastructure of the United States, intellectual prop-  
19 erty in the United States, and the privacy of citizens  
20 of the United States.

21          (5) A review of policy tools available to the  
22 President to deter and de-escalate tensions with for-  
23 eign countries, state-sponsored actors, and private  
24 actors regarding threats in cyberspace, and to what



1 degree such tools have been used and whether or not  
2 such tools have been effective.

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

6 (7) A clarification of the applicability of inter-  
7 national laws and norms, including the law of armed  
8 conflict, to the use of ICT.

9 (8) A clarification that countries that fall victim  
10 to malicious cyber activities have the right to take  
11 proportionate countermeasures under international  
12 law.

13 (c) FORM OF STRATEGY.—

14 (1) PUBLIC AVAILABILITY.—The strategy re-  
15 quired under subsection (a) shall be available to the  
16 public in unclassified form, including through publi-  
17 cation in the Federal Register.

18 (2) CLASSIFIED ANNEX.—

19 (A) IN GENERAL.—If the Secretary of  
20 State determines that such is appropriate, the  
21 strategy required under subsection (a) may in-  
22 clude a classified annex consistent with United  
23 States national security interests.

24 (B) RULE OF CONSTRUCTION.—Nothing in  
25 this subsection may be construed as authorizing

1           the public disclosure of an unclassified annex  
2           under subparagraph (A).

3           (d) BRIEFING.—Not later than 30 days after the pro-  
4           duction of the strategy required under subsection (a), the  
5           Secretary of State shall brief the Committee on Foreign  
6           Affairs of the House of Representatives and the Com-  
7           mittee on Foreign Relations of the Senate on such strat-  
8           egy, including any material contained in a classified  
9           annex.

10          (e) UPDATES.—The strategy required under sub-  
11          section (a) shall be updated—

12           (1) not later than 90 days after there has been  
13          any material change to United States policy as de-  
14          scribed in such strategy; and

15           (2) not later than one year after each inaugura-  
16          tion of a new President.

17          (f) PREEXISTING REQUIREMENT.—Upon the produc-  
18          tion and publication of the report required under section  
19          3(c) of the Presidential Executive Order 13800 on  
20          Strengthening the Cybersecurity of Federal Networks and  
21          Critical Infrastructure on May 11, 2017, such report shall  
22          be considered as satisfying the requirement under sub-  
23          section (a) of this section.

1 **SEC. 7. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS**  
2 **PRACTICES.**

3 (a) REPORT RELATING TO ECONOMIC ASSIST-  
4 ANCE.—Section 116 of the Foreign Assistance Act of  
5 1961 (22 U.S.C. 2151n) is amended by adding at the end  
6 the following new subsection:

7 “(h)(1) The report required by subsection (d) shall  
8 include an assessment of freedom of expression with re-  
9 spect to electronic information in each foreign country.  
10 Such assessment shall consist of the following:

11 “(A) An assessment of the general extent to  
12 which internet access is available to and used by citi-  
13 zens in each country.

14 “(B) An assessment of the extent to which gov-  
15 ernment authorities in each country attempt to fil-  
16 ter, censor, or otherwise block or remove nonviolent  
17 expression of political or religious opinion or belief  
18 via the internet, including electronic mail, as well as  
19 a description of the means by which such authorities  
20 attempt to block or remove protected speech.

21 “(C) An assessment of the extent to which gov-  
22 ernment authorities in each country have persecuted,  
23 prosecuted, or otherwise punished an individual or  
24 group for the nonviolent expression of political, reli-  
25 gious, or ideological opinion or belief via the inter-  
26 net, including electronic mail.

1           “(D) An assessment of the extent to which gov-  
2           ernment authorities in each country have sought to  
3           collect, request, obtain, or disclose the personally  
4           identifiable information of a person in connection  
5           with such person’s nonviolent expression of political,  
6           religious, or ideological opinion, belief, or commu-  
7           nication that would be protected by the International  
8           Covenant on Civil and Political Rights.

9           “(E) An assessment of the extent to which wire  
10          communications and electronic communications are  
11          monitored without regard to the principles of pri-  
12          vacy, human rights, democracy, and rule of law.

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

18          “(3) In this subsection—

19                 “(A) the term ‘electronic communication’ has  
20                 the meaning given such term in section 2510 of title  
21                 18, United States Code;

22                 “(B) the term ‘internet’ has the meaning given  
23                 such term in section 231(e)(3) of the Communica-  
24                 tions Act of 1934 (47 U.S.C. 231(e)(3));

1           “(C) the term ‘personally identifiable informa-  
2           tion’ means data in a form that identifies a par-  
3           ticular person; and

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

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

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

13           (2) by adding at the end the following new sub-  
14           section:

15           “(k)(1) The report required by subsection (b) shall  
16           include an assessment of freedom of expression with re-  
17           spect to electronic information in each foreign country.  
18           Such assessment shall consist of the following:

19           “(A) An assessment of the general extent to  
20           which internet access is available to and used by citi-  
21           zens in each country.

22           “(B) An assessment of the extent to which gov-  
23           ernment authorities in each country attempt to fil-  
24           ter, censor, or otherwise block or remove nonviolent  
25           expression of political or religious opinion or belief

1 via the internet, as well as a description of the  
2 means by which such authorities attempt to block or  
3 remove such expression.

4 “(C) An assessment of the extent to which gov-  
5 ernment authorities in each country have persecuted,  
6 prosecuted, or otherwise punished an individual or  
7 group for the peaceful expression of political, reli-  
8 gious, or ideological opinion or belief via the inter-  
9 net.

10 “(D) An assessment of the extent to which gov-  
11 ernment authorities in each country have sought to  
12 collect, request, obtain, or disclose personally identi-  
13 fiable information, or other information that could  
14 be used to classify individuals into a historically dis-  
15 criminated category based on a person’s nonviolent  
16 expression of political, religious, or ideological opin-  
17 ion or belief, including without limitation commu-  
18 nication that would be protected by the International  
19 Covenant on Civil and Political Rights.

20 “(E) An assessment of the extent to which wire  
21 communications and electronic communications are  
22 monitored without regard to the principles of pri-  
23 vacy, human rights, democracy, and rule of law.

24 “(2) In compiling data and making assessments for  
25 the purposes of paragraph (1), United States diplomatic

1 personnel shall consult with human rights organizations,  
2 technology and internet companies, and other appropriate  
3 nongovernmental organizations.

4 “(3) In this subsection—

5 “(A) the term ‘electronic communication’ has  
6 the meaning given such term in section 2510 of title  
7 18, United States Code;

8 “(B) the term ‘internet’ has the meaning given  
9 such term in section 231(e)(3) of the Communica-  
10 tions Act of 1934 (47 U.S.C. 231(e)(3));

11 “(C) the term ‘personally identifiable informa-  
12 tion’ means data in a form that identifies a par-  
13 ticular person; and

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