

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.

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

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Cyber Diplomacy Act
3 of 2017”.

4 **SEC. 2. FINDINGS.**

5 Congress finds the following:

6 (1) The stated goal of the United States Inter-
7 national Strategy for Cyberspace, launched on May
8 16, 2011, is to “work internationally to promote an
9 open, interoperable, secure, and reliable information
10 and communications infrastructure that supports
11 international trade and commerce, strengthens inter-
12 national security, and fosters free expression and in-
13 novation * * * in which norms of responsible behav-
14 ior guide States’ actions, sustain partnerships, and
15 support the rule of law in cyberspace.”.

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

1 (3) On January 13, 2015, China, Kazakhstan,
2 Kyrgyzstan, Russia, Tajikistan, and Uzbekistan pro-
3 posed a troubling international code of conduct for
4 information security which defines responsible State
5 behavior in cyberspace to include “curbing the dis-
6 semination of information” and the “right to inde-
7 pendent control of information and communications
8 technology” when a country’s political security is
9 threatened.

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

14 (5) On September 25, 2015, the United States
15 and China announced a commitment “that neither
16 country’s government will conduct or knowingly sup-
17 port cyber-enabled theft of intellectual property, in-
18 cluding trade secrets or other confidential business
19 information, with the intent of providing competitive
20 advantages to companies or commercial sectors.”.

21 (6) At the Antalya Summit from November 15–
22 16, 2015, the Group of 20 (G20) Leaders’ Commu-
23 nique affirmed the applicability of international law
24 to State behavior in cyberspace, called on States to
25 refrain from cyber-enabled theft of intellectual prop-

1 erty for commercial gain, and endorsed the view that
2 all States should abide by norms of responsible be-
3 havior.

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

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

16 (9) The 2017 Group of 7 (G7) Declaration on
17 Responsible States Behavior in Cyberspace recog-
18 nized on April 11, 2017, “the urgent necessity of in-
19 creased international cooperation to promote secu-
20 rity and stability in cyberspace * * * consisting of
21 the applicability of existing international law to
22 State behavior in cyberspace, the promotion of vol-
23 untary, non-binding norms of responsible State be-
24 havior during peacetime” and reaffirmed “that the

1 same rights that people have offline must also be
2 protected online.”.

3 (10) In testimony before the Select Committee
4 on Intelligence of the Senate on May 11, 2017, the
5 Director of National Intelligence identified six cyber
6 threat actors, including Russia for “efforts to influ-
7 ence the 2016 US election”; China, for “actively tar-
8 geting the US Government, its allies, and US com-
9 panies for cyber espionage”; Iran for “leverage[ing]
10 cyber espionage, propaganda, and attacks to support
11 its security priorities, influence events and foreign
12 perceptions, and counter threats”; North Korea for
13 “previously conduct[ing] cyber-attacks against US
14 commercial entities—specifically, Sony Pictures En-
15 tertainment in 2014”; terrorists, who “use the Inter-
16 net to organize, recruit, spread propaganda, raise
17 funds, collect intelligence, inspire action by followers,
18 and coordinate operations”; and criminals who “are
19 also developing and using sophisticated cyber tools
20 for a variety of purposes including theft, extortion,
21 and facilitation of other criminal activities”.

22 (11) On May 11, 2017, President Trump issued
23 Presidential Executive Order No. 13800 on
24 Strengthening the Cybersecurity of Federal Net-
25 works and Infrastructure which designated the Sec-

1 (b) IMPLEMENTATION.—In implementing the policy
2 described in subsection (a), the President, in consultation
3 with outside actors, including technology companies, non-
4 governmental organizations, security researchers, and
5 other relevant stakeholders, shall pursue the following ob-
6 jectives in the conduct of bilateral and multilateral rela-
7 tions:

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

11 (2) Clarifying that countries that fall victim to
12 malicious cyber activities have the right to take pro-
13 portionate countermeasures under international law,
14 provided such measures do not violate a funda-
15 mental human right or peremptory norm.

16 (3) Reducing and limiting the risk of escalation
17 and retaliation in cyberspace, such as massive de-
18 nial-of-service attacks, damage to critical infrastruc-
19 ture, or other malicious cyber activity that impairs
20 the use and operation of critical infrastructure that
21 provides services to the public.

22 (4) Cooperating with like-minded democratic
23 countries that share common values and cyberspace
24 policies with the United States, including respect for

1 human rights, democracy, and rule of law, to ad-
2 vance such values and policies internationally.

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

6 (A) Countries should not conduct or know-
7 ingly support cyber-enabled theft of intellectual
8 property, including trade secrets or other con-
9 fidential business information, with the intent
10 of providing competitive advantages to compa-
11 nies or commercial sectors.

12 (B) Countries should cooperate in devel-
13 oping and applying measures to increase sta-
14 bility and security in the use of ICTs and to
15 prevent ICT practices that are acknowledged to
16 be harmful or that may pose threats to inter-
17 national peace and security.

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

22 (D) Countries should not conduct or know-
23 ingly support ICT activity that, contrary to
24 international law, intentionally damages or oth-
25 erwise impairs the use and operation of critical

1 infrastructure, and should take appropriate
2 measures to protect their critical infrastructure
3 from ICT threats.

4 (E) Countries should not conduct or know-
5 ingly support malicious international activity
6 that, contrary to international law, harms the
7 information systems of authorized emergency
8 response teams (sometimes known as “com-
9 puter emergency response teams” or “cyberse-
10 curity incident response teams”) or related pri-
11 vate sector companies of another country.

12 (F) Countries should identify economic
13 drivers and incentives to promote securely-de-
14 signed ICT products and to develop policy and
15 legal frameworks to promote the development of
16 secure internet architecture.

17 (G) Countries should respond to appro-
18 priate requests for assistance to mitigate mali-
19 cious ICT activity aimed at the critical infra-
20 structure of another country emanating from
21 their territory.

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

1 (I) Countries should protect the exercise of
2 human rights and fundamental freedoms on the
3 Internet and commit to the principle that the
4 human rights that people have offline enjoy the
5 same protections online.

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

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

10 (1) by redesignating subsection (g) as sub-
11 section (h); and

12 (2) by inserting after subsection (f) the fol-
13 lowing new subsection:

14 “(g) OFFICE OF CYBER ISSUES.—

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

21 “(2) DUTIES.—

22 “(A) IN GENERAL.—The head of the Of-
23 fice shall perform such duties and exercise such
24 powers as the Secretary of State shall prescribe,
25 including implementing the policy of the United

1 States described in section 3 of the Cyber Di-
2 plomacy Act of 2017.

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

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

9 “(ii) lead the Department of State’s
10 diplomatic cyberspace efforts generally, in-
11 cluding relating to international cybersecu-
12 rity, internet access, internet freedom, dig-
13 ital economy, cybercrime, deterrence and
14 international responses to cyber threats;

15 “(iii) promote an open, interoperable,
16 reliable, unfettered, and secure information
17 and communications technology infrastruc-
18 ture globally;

19 “(iv) represent the Secretary of State
20 in interagency efforts to develop and ad-
21 vance the United States international
22 cyberspace policy;

23 “(v) coordinate within the Depart-
24 ment of State and with other components
25 of the United States Government cyber-

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

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

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

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

12 “(B) international diplomacy.

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

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

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

21 “(B) the head of the Office from being ele-
22 vated to an Assistant Secretary, if such an As-
23 sistant Secretary position does not increase the
24 number of Assistant Secretary positions at the

1 Department above the number authorized under
2 subsection (c)(1).”.

3 (b) SENSE OF CONGRESS.—It is the sense of Con-
4 gress that the Office of Cyber Issues established under
5 section 1(g) of the State Department Basic Authorities
6 Act of 1956 (as amended by subsection (a) of this section)
7 should be a Bureau of the Department of State headed
8 by an Assistant Secretary, subject to the rule of construc-
9 tion specified in paragraph (5)(B) of such section 1(g).

10 (c) UNITED NATIONS.—The Permanent Representa-
11 tive of the United States to the United Nations shall use
12 the voice, vote, and influence of the United States to op-
13 pose any measure that is inconsistent with the United
14 States international cyberspace policy described in section
15 3.

16 **SEC. 5. INTERNATIONAL CYBERSPACE EXECUTIVE AR-**
17 **RANGEMENTS.**

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

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

1 mitted to the Committee on Foreign Affairs of the House
2 of Representatives and the Committee on Foreign Rela-
3 tions of the Senate not later than 5 days after such ar-
4 rangement is signed or otherwise agreed to, together with
5 an explanation of such arrangement, its purpose, how such
6 arrangement is consistent with the United States inter-
7 national cyberspace policy described in section 3, and how
8 such arrangement will be implemented.

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

1 (d) EXISTING EXECUTIVE ARRANGEMENTS.—Not
2 later than 60 days after the date of the enactment of this
3 Act, the President shall satisfy the requirements of sub-
4 section (c) for the following executive arrangements al-
5 ready in effect:

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

8 (2) The arrangement announced between the
9 United States and the United Kingdom on January
10 16, 2015.

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

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

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

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

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

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

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

1 (10) Any other similar bilateral or multilateral
2 arrangement announced before the date of the en-
3 actment of this Act.

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

5 (a) **STRATEGY REQUIRED.**—Not later than 1 year
6 after the date of the enactment of this Act, the Secretary
7 of State, in coordination with the heads of other relevant
8 Federal departments and agencies, shall produce a strat-
9 egy relating to United States international policy with re-
10 gard to cyberspace.

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

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

16 (2) A plan of action to guide the diplomacy of
17 the Department of State with regard to foreign
18 countries, including conducting bilateral and multi-
19 lateral activities to develop the norms of responsible
20 international behavior in cyberspace, and status re-
21 view of existing efforts in multilateral fora to obtain
22 agreements on international norms in cyberspace.

23 (3) A review of alternative concepts with regard
24 to international norms in cyberspace offered by for-
25 eign countries.

1 (4) A detailed description of new and evolving
2 threats to United States national security in cyber-
3 space from foreign countries, State-sponsored actors,
4 and private actors to Federal and private sector in-
5 frastructure of the United States, intellectual prop-
6 erty in the United States, and the privacy of citizens
7 of the United States.

8 (5) A review of policy tools available to the
9 President to deter and de-escalate tensions with for-
10 eign countries, State-sponsored actors, and private
11 actors regarding threats in cyberspace, and to what
12 degree such tools have been used and whether or not
13 such tools have been effective.

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

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

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

1 (9) A plan of action to guide the diplomacy of
2 the Department of State with regard to existing mu-
3 tual defense agreements, including the inclusion in
4 such agreements of information relating to the appli-
5 cability of malicious cyber activities in triggering
6 mutual defense obligations.

7 (c) FORM OF STRATEGY.—

8 (1) PUBLIC AVAILABILITY.—The strategy re-
9 quired under subsection (a) shall be available to the
10 public in unclassified form, including through publi-
11 cation in the Federal Register.

12 (2) CLASSIFIED ANNEX.—

13 (A) IN GENERAL.—If the Secretary of
14 State determines that such is appropriate, the
15 strategy required under subsection (a) may in-
16 clude a classified annex consistent with United
17 States national security interests.

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

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

1 mittee on Foreign Relations of the Senate on such strat-
2 egy, including any material contained in a classified
3 annex.

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

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

9 (2) not later than 1 year after each inaugura-
10 tion of a new President.

11 (f) PREEXISTING REQUIREMENT.—Upon the produc-
12 tion and publication of the report required under section
13 3(c) of the Presidential Executive Order No. 13800 on
14 Strengthening the Cybersecurity of Federal Networks and
15 Critical Infrastructure on May 11, 2017, such report shall
16 be considered as satisfying the requirement under sub-
17 section (a) of this section.

18 **SEC. 7. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS**

19 **PRACTICES.**

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

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

1 spect to electronic information in each foreign country.

2 Such assessment shall consist of the following:

3 “(A) An assessment of the extent to which gov-
4 ernment authorities in each country inappropriately
5 attempt to filter, censor, or otherwise block or re-
6 move nonviolent expression of political or religious
7 opinion or belief via the internet, including electronic
8 mail, as well as a description of the means by which
9 such authorities attempt to block or remove such ex-
10 pression.

11 “(B) An assessment of the extent to which gov-
12 ernment authorities in each country have persecuted
13 or otherwise punished an individual or group for the
14 nonviolent expression of political, religious, or ideo-
15 logical opinion or belief via the internet, including
16 electronic mail.

17 “(C) An assessment of the extent to which gov-
18 ernment authorities in each country have sought to
19 inappropriately collect, request, obtain, or disclose
20 personally identifiable information of a person in
21 connection with such person’s nonviolent expression
22 of political, religious, or ideological opinion or belief,
23 including expression that would be protected by the
24 International Covenant on Civil and Political Rights.

1 “(D) An assessment of the extent to which wire
2 communications and electronic communications are
3 monitored without regard to the principles of pri-
4 vacy, human rights, democracy, and rule of law.

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

10 “(3) In this subsection—

11 “(A) the term ‘electronic communication’ has
12 the meaning given such term in section 2510 of title
13 18, United States Code;

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

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

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

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

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

4 (2) by adding at the end the following new sub-
5 section:

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

10 “(A) An assessment of the extent to which gov-
11 ernment authorities in each country inappropriately
12 attempt to filter, censor, or otherwise block or re-
13 move nonviolent expression of political or religious
14 opinion or belief via the internet, including electronic
15 mail, as well as a description of the means by which
16 such authorities attempt to block or remove such ex-
17 pression.

18 “(B) An assessment of the extent to which gov-
19 ernment authorities in each country have persecuted
20 or otherwise punished an individual or group for the
21 nonviolent expression of political, religious, or ideo-
22 logical opinion or belief via the internet, including
23 electronic mail.

24 “(C) An assessment of the extent to which gov-
25 ernment authorities in each country have sought to

1 inappropriately collect, request, obtain, or disclose
2 personally identifiable information of a person in
3 connection with such person’s nonviolent expression
4 of political, religious, or ideological opinion or belief,
5 including expression that would be protected by the
6 International Covenant on Civil and Political Rights.

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

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

16 “(3) In this subsection—

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

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

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

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

 Passed the House of Representatives January 17,
2018.

Attest:

KAREN L. HAAS,

Clerk.