

Calendar No. 495

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

JUNE 28, 2018

Reported by Mr. CORKER, with an amendment

[Strike out all after the enacting clause and insert the part printed in italics]

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,*

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 behav-
7 ior guide States’ actions, sustain partnerships, and
8 support 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
15 the applicability of existing international law to
16 State behavior in cyberspace, the promotion of vol-
17 untary, non-binding norms of responsible State be-
18 havior during peacetime” and reaffirmed “that the
19 same rights that people have offline must also be
20 protected 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 No. 13800 on
17 Strengthening the Cybersecurity of Federal Net-
18 works and Infrastructure which designated the Sec-
19 retary of State to lead an interagency effort to de-
20 velop strategic options for the President to deter ad-
21 versaries from cyber threats and an engagement
22 strategy for international cooperation in cybersecu-
23 rity, noting that “the United States is especially de-
24 pendent on a globally secure and resilient internet
25 and must work with allies and other partners” to

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

4 (2) Clarifying that countries that fall victim to
5 malicious cyber activities have the right to take pro-
6 portionate countermeasures under international law,
7 provided such measures do not violate a funda-
8 mental human right or peremptory norm.

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

15 (4) Cooperating with like-minded democratic
16 countries that share common values and cyberspace
17 policies with the United States, including respect for
18 human rights, democracy, and rule of law, to ad-
19 vance such values and policies internationally.

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

23 (A) Countries should not conduct or know-
24 ingly support cyber-enabled theft of intellectual
25 property, including trade secrets or other con-

1 fidential business information, with the intent
2 of providing competitive advantages to compa-
3 nies or commercial sectors.

4 (B) Countries should cooperate in devel-
5 oping and applying measures to increase sta-
6 bility and security in the use of ICTs and to
7 prevent ICT practices that are acknowledged to
8 be harmful or that may pose threats to inter-
9 national peace and security.

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

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

21 (E) Countries should not conduct or know-
22 ingly support malicious international activity
23 that, contrary to international law, harms the
24 information systems of authorized emergency
25 response teams (sometimes known as “com-

1 puter emergency response teams” or “cyberse-
2 curity incident response teams”) or related pri-
3 vate sector companies of another country.

4 (F) Countries should identify economic
5 drivers and incentives to promote securely-de-
6 signed ICT products and to develop policy and
7 legal frameworks to promote the development of
8 secure internet architecture.

9 (G) Countries should respond to appro-
10 priate requests for assistance to mitigate mali-
11 cious ICT activity aimed at the critical infra-
12 structure of another country emanating from
13 their territory.

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

17 (I) Countries should protect the exercise of
18 human rights and fundamental freedoms on the
19 Internet and commit to the principle that the
20 human rights that people have offline enjoy the
21 same protections online.

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

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

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

3 (2) by inserting after subsection (f) the fol-
4 lowing new subsection:

5 “(g) OFFICE OF CYBER ISSUES.—

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

12 “(2) DUTIES.—

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

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

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

1 “(ii) lead the Department of State’s
2 diplomatic cyberspace efforts generally, in-
3 cluding relating to international cybersecu-
4 rity, internet access, internet freedom, dig-
5 ital economy, cybercrime, deterrence and
6 international responses to cyber threats;

7 “(iii) promote an open, interoperable,
8 reliable, unfettered, and secure information
9 and communications technology infrastruc-
10 ture globally;

11 “(iv) represent the Secretary of State
12 in interagency efforts to develop and ad-
13 vance the United States international
14 cyberspace policy;

15 “(v) coordinate within the Depart-
16 ment of State and with other components
17 of the United States Government cyber-
18 space efforts and other relevant functions,
19 including countering terrorists’ use of
20 cyberspace; and

21 “(vi) act as liaison to public and pri-
22 vate sector entities on relevant cyberspace
23 issues.

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

4 “(A) cybersecurity and other relevant cyber
5 issues; and

6 “(B) international diplomacy.

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

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

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

15 “(B) the head of the Office from being ele-
16 vated to an Assistant Secretary, if such an As-
17 sistant Secretary position does not increase the
18 number of Assistant Secretary positions at the
19 Department above the number authorized under
20 subsection (e)(1).”.

21 (b) SENSE OF CONGRESS.—It is the sense of Con-
22 gress that the Office of Cyber Issues established under
23 section 1(g) of the State Department Basic Authorities
24 Act of 1956 (as amended by subsection (a) of this section)
25 should be a Bureau of the Department of State headed

1 by an Assistant Secretary, subject to the rule of construc-
2 tion specified in paragraph (5)(B) of such section 1(g).

3 (c) UNITED NATIONS.—The Permanent Representa-
4 tive of the United States to the United Nations shall use
5 the voice, vote, and influence of the United States to op-
6 pose any measure that is inconsistent with the United
7 States international cyberspace policy described in section
8 3.

9 **SEC. 5. INTERNATIONAL CYBERSPACE EXECUTIVE AR-**
10 **RANGEMENTS.**

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

15 (b) TRANSMISSION TO CONGRESS.—The text of any
16 executive arrangement (including the text of any oral ar-
17 rangement, which shall be reduced to writing) entered into
18 by the United States under subsection (a) shall be trans-
19 mitted to the Committee on Foreign Affairs of the House
20 of Representatives and the Committee on Foreign Rela-
21 tions of the Senate not later than 5 days after such ar-
22 rangement is signed or otherwise agreed to, together with
23 an explanation of such arrangement, its purpose, how such
24 arrangement is consistent with the United States inter-

1 national cyberspace policy described in section 3, and how
2 such arrangement will be implemented.

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

19 (d) EXISTING EXECUTIVE ARRANGEMENTS.—Not
20 later than 60 days after the date of the enactment of this
21 Act, the President shall satisfy the requirements of sub-
22 section (c) for the following executive arrangements al-
23 ready in effect:

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

1 (2) The arrangement announced between the
2 United States and the United Kingdom on January
3 16, 2015.

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

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

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

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

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

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

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

18 (10) Any other similar bilateral or multilateral
19 arrangement announced before the date of the en-
20 actment of this Act.

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

22 (a) STRATEGY REQUIRED.—Not later than 1 year
23 after the date of the enactment of this Act, the Secretary
24 of State, in coordination with the heads of other relevant
25 Federal departments and agencies, shall produce a strat-

1 egy relating to United States international policy with re-
2 gard to cyberspace.

3 (b) ELEMENTS.—The strategy required under sub-
4 section (a) shall include the following:

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

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

15 (3) A review of alternative concepts with regard
16 to international norms in cyberspace offered by for-
17 eign countries.

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

1 (5) A review of policy tools available to the
2 President to deter and de-escalate tensions with for-
3 eign countries, State-sponsored actors, and private
4 actors regarding threats in cyberspace, and to what
5 degree such tools have been used and whether or not
6 such tools have been effective.

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

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

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

18 (9) A plan of action to guide the diplomacy of
19 the Department of State with regard to existing mu-
20 tual defense agreements, including the inclusion in
21 such agreements of information relating to the appli-
22 cability of malicious cyber activities in triggering
23 mutual defense obligations.

24 (c) FORM OF STRATEGY.—

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

5 (2) CLASSIFIED ANNEX.—

6 (A) IN GENERAL.—If the Secretary of
7 State determines that such is appropriate, the
8 strategy required under subsection (a) may in-
9 clude a classified annex consistent with United
10 States national security interests.

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

15 (d) BRIEFING.—Not later than 30 days after the pro-
16 duction of the strategy required under subsection (a), the
17 Secretary of State shall brief the Committee on Foreign
18 Affairs of the House of Representatives and the Com-
19 mittee on Foreign Relations of the Senate on such strat-
20 egy, including any material contained in a classified
21 annex.

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

1 move nonviolent expression of political or religious
2 opinion or belief via the internet, including electronic
3 mail, as well as a description of the means by which
4 such authorities attempt to block or remove such ex-
5 pression.

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

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

20 “(D) 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.”.

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

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

23 (2) by adding at the end the following new sub-
24 section:

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

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

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

19 “(C) An assessment of the extent to which gov-
20 ernment authorities in each country have sought to
21 inappropriately collect, request, obtain, or disclose
22 personally identifiable information of a person in
23 connection with such person’s nonviolent expression
24 of political, religious, or ideological opinion or belief,

1 including expression that would be protected by the
2 International Covenant on Civil and Political Rights.

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

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

12 “(3) In this subsection—

13 “(A) the term ‘electronic communication’ has
14 the meaning given such term in section 2510 of title
15 18, United States Code;

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

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

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

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) *SHORT TITLE.*—*This Act may be cited as the*
 3 *“Cyber Diplomacy Act of 2018”.*

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

Sec. 1. Short title; table of contents.

Sec. 2. Findings.

Sec. 3. Definitions.

Sec. 4. United States International Cyberspace Policy.

Sec. 5. Department of State responsibilities.

Sec. 6. International cyberspace executive arrangements.

Sec. 7. International strategy for cyberspace.

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

Sec. 9. GAO report on cyber threats and data misuse.

*Sec. 10. Sense of Congress on cybersecurity sanctions against North Korea and
 cybersecurity legislation in Vietnam.*

6 **SEC. 2. FINDINGS.**

7 *Congress makes the following findings:*

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

18 (2) *In its June 24, 2013 report, the Group of*
 19 *Governmental Experts on Developments in the Field*
 20 *of Information and Telecommunications in the Con-*

1 *text of International Security (referred to in this sec-*
2 *tion as “GGE”), established by the United Nations*
3 *General Assembly, concluded that “State sovereignty*
4 *and the international norms and principles that flow*
5 *from it apply to States’ conduct of [information and*
6 *communications technology] ICT-related activities*
7 *and to their jurisdiction over ICT infrastructure with*
8 *their territory”.*

9 (3) *In January 2015, China, Kazakhstan,*
10 *Kyrgyzstan, Russia, Tajikistan, and Uzbekistan pro-*
11 *posed a troubling international code of conduct for*
12 *information security, which could be used as a pretext*
13 *for restricting political dissent, and includes “curbing*
14 *the dissemination of information that incites ter-*
15 *rorism, separatism or extremism or that inflames ha-*
16 *tred on ethnic, racial or religious grounds”.*

17 (4) *In its July 22, 2015 consensus report, GGE*
18 *found that “norms of responsible State behavior can*
19 *reduce risks to international peace, security and sta-*
20 *bility”.*

21 (5) *On September 25, 2015, the United States*
22 *and China announced a commitment that neither*
23 *country’s government “will conduct or knowingly*
24 *support cyber-enabled theft of intellectual property,*
25 *including trade secrets or other confidential business*

1 *information, with the intent of providing competitive*
2 *advantages to companies or commercial sectors”.*

3 *(6) At the Antalya Summit on November 15 and*
4 *16, 2015, the Group of 20 Leaders’ communiqué—*

5 *(A) affirmed the applicability of inter-*
6 *national law to state behavior in cyberspace;*

7 *(B) called on states to refrain from cyber-*
8 *enabled theft of intellectual property for commer-*
9 *cial gain; and*

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

12 *(7) The March 2016 Department of State Inter-*
13 *national Cyberspace Policy Strategy noted that “the*
14 *Department of State anticipates a continued increase*
15 *and expansion of our cyber-focused diplomatic efforts*
16 *for the foreseeable future”.*

17 *(8) On December 1, 2016, the Commission on*
18 *Enhancing National Cybersecurity, which was estab-*
19 *lished within the Department of Commerce by Execu-*
20 *tive Order 13718 (81 Fed. Reg. 7441), recommended*
21 *that “the President should appoint an Ambassador*
22 *for Cybersecurity to lead U.S. engagement with the*
23 *international community on cybersecurity strategies,*
24 *standards, and practices”.*

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

2
3
4 (A) *recognized “the urgent necessity of increased international cooperation to promote security and stability in cyberspace”;*

5
6
7 (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

8
9
10
11
12
13
14
15
16
17 (C) *reaffirmed that “the same rights that people have offline must also be protected online”.*

18
19
20 (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—*

21
22
23
24 (A) *Russia, for “efforts to influence the 2016 US election”;*

25

1 (B) China, for “actively targeting the US
2 Government, its allies, and US companies for
3 cyber espionage”;

4 (C) Iran, for “leverag[ing] cyber espionage,
5 propaganda, and attacks to support its security
6 priorities, influence events and foreign percep-
7 tions, and counter threats”;

8 (D) North Korea, for “previously
9 conduct[ing] cyber-attacks against US commer-
10 cial entities—specifically, Sony Pictures Enter-
11 tainment in 2014”;

12 (E) terrorists, who “use the Internet to or-
13 ganize, recruit, spread propaganda, raise funds,
14 collect intelligence, inspire action by followers,
15 and coordinate operations”; and

16 (F) criminals, who “are also developing and
17 using sophisticated cyber tools for a variety of
18 purposes including theft, extortion, and facilita-
19 tion of other criminal activities”.

20 (11) On May 11, 2017, President Donald J.
21 Trump issued Executive Order 13800 (82 Fed. Reg.
22 22391), entitled “Strengthening the Cybersecurity of
23 Federal Networks and Infrastructure”, which—

24 (A) designates the Secretary of State to lead
25 an interagency effort to develop an engagement

1 *strategy for international cooperation in cyberse-*
2 *curity; and*

3 *(B) notes that “the United States is espe-*
4 *cially dependent on a globally secure and resil-*
5 *ient internet and must work with allies and*
6 *other partners toward maintaining ... the policy*
7 *of the executive branch to promote an open,*
8 *interoperable, reliable, and secure internet that*
9 *fosters efficiency, innovation, communication,*
10 *and economic prosperity, while respecting pri-*
11 *vacv and guarding against disruption, fraud,*
12 *and theft”.*

13 **SEC. 3. DEFINITIONS.**

14 *In this Act:*

15 (1) *APPROPRIATE CONGRESSIONAL COMMIT-*
16 *TEES.—The term “appropriate congressional commit-*
17 *tees” means the Committee on Foreign Relations of*
18 *the Senate and the Committee on Foreign Affairs of*
19 *the House of Representatives.*

20 (2) *INFORMATION AND COMMUNICATIONS TECH-*
21 *NOLOGY; ICT.—The terms “information and commu-*
22 *nications technology” and “ICT” include hardware,*
23 *software, and other products or services primarily in-*
24 *tended to fulfill or enable the function of information*
25 *processing and communication by electronic means,*

1 *impairs the use and operation of critical infrastruc-*
2 *ture that provides services to the public.*

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

8 (4) *Encouraging the responsible development of*
9 *new, innovative technologies and ICT products that*
10 *strengthen a secure Internet architecture that is acces-*
11 *sible to all.*

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

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

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

1 (C) Countries should not conduct or know-
2 ingly support ICT activity that, contrary to
3 international law, intentionally damages or oth-
4 erwise impairs the use and operation of critical
5 infrastructure providing services to the public,
6 and should take appropriate measures to protect
7 their critical infrastructure from ICT threats.

8 (D) Countries should not conduct or know-
9 ingly support malicious international activity
10 that, contrary to international law, harms the
11 information systems of authorized emergency re-
12 sponse teams (also known as “computer emer-
13 gency response teams” or “cybersecurity incident
14 response teams”) of another country or authorize
15 emergency response teams to engage in malicious
16 international activity.

17 (E) Countries should respond to appro-
18 priate requests for assistance to mitigate mali-
19 cious ICT activity emanating from their terri-
20 tory and aimed at the critical infrastructure of
21 another country.

22 (F) Countries should not restrict cross-bor-
23 der data flows or require local storage or proc-
24 essing of data.

1 (G) 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 should also
 5 be protected online.

6 (6) Advancing, encouraging, and supporting the
 7 development and adoption of internationally recog-
 8 nized technical standards and best practices.

9 **SEC. 5. DEPARTMENT OF STATE RESPONSIBILITIES.**

10 (a) OFFICE OF CYBERSPACE AND THE DIGITAL ECON-
 11 OMY.—Section 1 of the State Department Basic Authorities
 12 Act of 1956 (22 U.S.C. 2651a) is amended—

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

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

16 “(g) OFFICE OF CYBERSPACE AND THE DIGITAL ECON-
 17 OMY.—

18 “(1) IN GENERAL.—There is established, within
 19 the Department of State, an Office of Cyberspace and
 20 the Digital Economy (referred to in this subsection as
 21 the ‘Office’). The head of the Office shall have the rank
 22 and status of ambassador and shall be appointed by
 23 the President, by and with the advice and consent of
 24 the Senate.

25 “(2) DUTIES.—

1 “(A) *IN GENERAL.*—*The head of the Office*
2 *shall perform such duties and exercise such pow-*
3 *ers as the Secretary of State shall prescribe, in-*
4 *cluding implementing the policy of the United*
5 *States described in section 4 of the Cyber Diplo-*
6 *macy Act of 2018.*

7 “(B) *DUTIES DESCRIBED.*—*The principal*
8 *duties and responsibilities of the head of the Of-*
9 *fice shall be—*

10 “(i) *to serve as the principal cyber pol-*
11 *icy official within the senior management of*
12 *the Department of State and as the advisor*
13 *to the Secretary of State for cyber issues;*

14 “(ii) *to lead the Department of State’s*
15 *diplomatic cyberspace efforts, including ef-*
16 *forts relating to international cybersecurity,*
17 *Internet access, Internet freedom, digital*
18 *economy, cybercrime, deterrence and inter-*
19 *national responses to cyber threats, and*
20 *other issues that the Secretary assigns to the*
21 *Office;*

22 “(iii) *to promote an open, interoper-*
23 *able, reliable, unfettered, and secure infor-*
24 *mation and communications technology in-*
25 *frastructure globally;*

1 “(iv) to represent the Secretary of
2 State in interagency efforts to develop and
3 advance the policy described in section 4 of
4 the Cyber Diplomacy Act of 2018;

5 “(v) to coordinate cyberspace efforts
6 and other relevant functions, including
7 countering terrorists’ use of cyberspace,
8 within the Department of State and with
9 other components of the United States Gov-
10 ernment;

11 “(vi) to act as a liaison to public and
12 private sector entities on relevant cyber-
13 space issues;

14 “(vii) to lead United States Govern-
15 ment efforts to establish a global deterrence
16 framework;

17 “(viii) to develop and execute adver-
18 sary-specific strategies to influence adver-
19 sary decisionmaking through the imposition
20 of costs and deterrence strategies;

21 “(ix) to advise the Secretary and co-
22 ordinate with foreign governments on exter-
23 nal responses to national-security-level
24 cyber incidents, including coordination on
25 diplomatic response efforts to support allies

1 *threatened by malicious cyber activity, in*
2 *conjunction with members of the North At-*
3 *lantic Treaty Organization and other like-*
4 *minded countries;*

5 *“(x) to promote the adoption of na-*
6 *tional processes and programs that enable*
7 *threat detection, prevention, and response to*
8 *malicious cyber activity emanating from*
9 *the territory of a foreign country, including*
10 *as such activity relates to the United States’*
11 *European allies, as appropriate;*

12 *“(xi) to promote the building of foreign*
13 *capacity to protect the global network with*
14 *the goal of enabling like-minded participa-*
15 *tion in deterrence frameworks;*

16 *“(xii) to promote the maintenance of*
17 *an open and interoperable Internet gov-*
18 *erned by the multi-stakeholder model, in-*
19 *stead of by centralized government control;*

20 *“(xiii) to promote an international*
21 *regulatory environment for technology in-*
22 *vestments and the Internet that benefits*
23 *United States economic and national secu-*
24 *rity interests;*

1 “(xiv) to promote cross-border flow of
2 data and combat international initiatives
3 seeking to impose unreasonable require-
4 ments on United States businesses;

5 “(xv) to promote international policies
6 to protect the integrity of United States and
7 international telecommunications infra-
8 structure from foreign-based, cyber-enabled
9 threats;

10 “(xvi) to serve as the interagency coor-
11 dinator for the United States Government
12 on engagement with foreign governments on
13 cyberspace and digital economy issues as
14 described in the Cyber Diplomacy Act of
15 2018;

16 “(xvii) to promote international poli-
17 cies to secure radio frequency spectrum for
18 United States businesses and national secu-
19 rity needs;

20 “(xviii) to promote and protect the ex-
21 ercise of human rights, including freedom of
22 speech and religion, through the Internet;

23 “(xix) to build capacity of United
24 States diplomatic officials to engage on
25 cyber issues;

1 “(xx) to encourage the development and
2 adoption by foreign countries of inter-
3 nationally recognized standards, policies,
4 and best practices; and

5 “(xvi) to promote and advance inter-
6 national policies that protect individuals’
7 private data.

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

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

13 “(B) international diplomacy.

14 “(4) ORGANIZATIONAL PLACEMENT.—During the
15 4-year period beginning on the date of the enactment
16 of the Cyber Diplomacy Act of 2018, the head of the
17 Office shall report to the Under Secretary for Polit-
18 ical Affairs or to an official holding a higher position
19 than the Under Secretary for Political Affairs in the
20 Department of State. After the conclusion of such pe-
21 riod, the head of the Office shall report to an appro-
22 priate Under Secretary or to an official holding a
23 higher position than Under Secretary.

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

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

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

5 (2) *in subsection (e)(2)(B), by adding at the end*
6 *the following:*

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

9 (3) *by redesignating subsection (f) as subsection*
10 *(g); and*

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

12 “*(f) With respect to any bilateral or multilateral cyber-*
13 *space agreement under subsection (e)(2)(B)(iii) and the in-*
14 *formation required to be transmitted to Congress under sub-*
15 *section (a), or with respect to any arrangement that seeks*
16 *to secure commitments on responsible country behavior in*
17 *cyberspace consistent with section 4(b)(5) of the Cyber Di-*
18 *plomacy Act of 2018, the Secretary of State shall provide*
19 *an explanation of such arrangement, including—*

20 “*(1) the purpose of such arrangement;*

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

23 “*(3) how such arrangement will be imple-*
24 *mented.*”.

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

7 (1) notify the appropriate congressional commit-
8 tees if another country fails to meet the commitments
9 contained in such agreement; and

10 (2) describe the steps that the United States has
11 taken or plans to take to ensure that all such commit-
12 ments are fulfilled.

13 (d) *EXISTING EXECUTIVE ARRANGEMENTS*.—Not later
14 than 180 days after the date of the enactment of this Act,
15 the Secretary of State shall brief the appropriate congres-
16 sional committees regarding any executive bilateral or mul-
17 tilateral cyberspace arrangement in effect before the date
18 of enactment of this Act, including—

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) *the arrangement announced between the*
14 *United States and France on February 9, 2018;*

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

17 (12) *any other similar bilateral or multilateral*
18 *arrangement announced before such date of enact-*
19 *ment.*

20 **SEC. 7. INTERNATIONAL STRATEGY FOR CYBERSPACE.**

21 (a) *STRATEGY REQUIRED.*—*Not later than 1 year*
22 *after the date of the enactment of this Act, the President,*
23 *acting through the Secretary of State, and in coordination*
24 *with the heads of other relevant Federal departments and*
25 *agencies, shall develop a strategy relating to United States*

1 *engagement with foreign governments on international*
2 *norms with respect to responsible state behavior in cyber-*
3 *space.*

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

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

8 (2) *A plan of action to guide the diplomacy of*
9 *the Department of State with regard to foreign coun-*
10 *tries, including—*

11 (A) *conducting bilateral and multilateral*
12 *activities to develop norms of responsible country*
13 *behavior in cyberspace consistent with the objec-*
14 *tives under section 4(b)(5); and*

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

19 (3) *A review of alternative concepts with regard*
20 *to international norms in cyberspace offered by for-*
21 *foreign countries.*

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

25 (A) *United States national security;*

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

3 (C) *intellectual property in the United*
4 *States; and*

5 (D) *the privacy of citizens of the United*
6 *States.*

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

13 (6) *A review of resources required to conduct ac-*
14 *tivities to build responsible norms of international*
15 *cyber behavior.*

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

21 (c) *FORM OF STRATEGY.—*

22 (1) *PUBLIC AVAILABILITY.—The strategy re-*
23 *quired under subsection (a) shall be available to the*
24 *public in unclassified form, including through publi-*
25 *cation in the Federal Register.*

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

6 (d) *BRIEFING.*—*Not later than 30 days after the com-*
7 *pletion of the strategy required under subsection (a), the*
8 *Secretary of State shall brief the appropriate congressional*
9 *committees on the strategy, including any material con-*
10 *tained in a classified annex.*

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

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

16 (2) *not later than 1 year after the inauguration*
17 *of each new President.*

18 (f) *PREEXISTING REQUIREMENT.*—*The Recommenda-*
19 *tions to the President on Protecting American Cyber Inter-*
20 *ests through International Engagement, prepared by the Of-*
21 *fice of the Coordinator for Cyber Issues on May 31, 2018,*
22 *pursuant to section 3(c) of Executive Order 13800 (82 Fed.*
23 *Reg. 22391), shall be deemed to satisfy the requirement*
24 *under subsection (a).*

1 **SEC. 8. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS**
2 **PRACTICES.**

3 *Section 116 of the Foreign Assistance Act of 1961 (22*
4 *U.S.C. 2151n) is amended by adding at the end the fol-*
5 *lowing:*

6 *“(h)(1) The report required under subsection (d) shall*
7 *include an assessment of freedom of expression with respect*
8 *to electronic information in each foreign country that in-*
9 *cludes the following:*

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

18 *“(B) An assessment of the extent to which gov-*
19 *ernment authorities in the country have persecuted or*
20 *otherwise punished, arbitrarily and without due proc-*
21 *ess, an individual or group for the nonviolent expres-*
22 *sion of political, religious, or ideological opinion or*
23 *belief through the Internet, including electronic mail.*

24 *“(C) An assessment of the extent to which gov-*
25 *ernment authorities in the country have sought, inap-*
26 *propriately and with malicious intent, to collect, re-*

1 *quest, obtain, or disclose without due process person-*
2 *ally identifiable information of a person in connec-*
3 *tion with that person’s nonviolent expression of polit-*
4 *ical, religious, or ideological opinion or belief, includ-*
5 *ing expression that would be protected by the Inter-*
6 *national Covenant on Civil and Political Rights,*
7 *adopted at New York December 16, 1966, and entered*
8 *into force March 23, 1976, as interpreted by the*
9 *United States.*

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

15 *“(2) In compiling data and making assessments under*
16 *paragraph (1), United States diplomatic personnel should*
17 *consult with relevant entities, including human rights orga-*
18 *nizations, the private sector, the governments of like-minded*
19 *countries, technology and Internet companies, and other ap-*
20 *propriate nongovernmental organizations or entities.*

21 *“(3) In this subsection—*

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

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

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

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

10 **SEC. 9. GAO REPORT ON CYBER THREATS AND DATA MIS-**
11 **USE.**

12 *Not later than 1 year after the date of the enactment*
13 *of this Act, the Comptroller General of the United States*
14 *shall submit a report and provide a briefing to the appro-*
15 *priate congressional committees that includes—*

16 (1) *a description of the primary threats to the*
17 *personal information of United States citizens from*
18 *international actors within the cyberspace domain;*

19 (2) *an assessment of the extent to which United*
20 *States diplomatic processes and other efforts with for-*
21 *oreign countries, including through multilateral fora,*
22 *bilateral engagements, and negotiated cyberspace*
23 *agreements, strengthen the protections of United*
24 *States citizens’ personal information;*

1 (3) *an assessment of the Department of State’s*
2 *report in response to Executive Order 13800 (82 Fed.*
3 *Reg. 22391), which documents an engagement strat-*
4 *egy for international cooperation in cybersecurity and*
5 *the extent to which this strategy addresses protections*
6 *of United States citizens’ personal information;*

7 (4) *recommendations for United States policy-*
8 *makers on methods to properly address and strength-*
9 *en the protections of United States citizens’ personal*
10 *information from misuse by international actors; and*

11 (5) *any other matters deemed relevant by the*
12 *Comptroller General.*

13 **SEC. 10. SENSE OF CONGRESS ON CYBERSECURITY SANC-**
14 **TIONS AGAINST NORTH KOREA AND CYBER-**
15 **SECURITY LEGISLATION IN VIETNAM.**

16 *It is the sense of Congress that—*

17 (1) *the President should designate all entities*
18 *that knowingly engage in significant activities under-*
19 *mining cybersecurity through the use of computer net-*
20 *works or systems against foreign persons, govern-*
21 *ments, or other entities on behalf of the Government*
22 *of North Korea, consistent with section 209(b) of the*
23 *North Korea Sanctions and Policy Enhancement Act*
24 *of 2016 (22 U.S.C. 9229(b));*

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

3 (A) *may not be consistent with inter-*
4 *national trade standards; and*

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

7 (3) *the Government of Vietnam should—*

8 (A) *delay the implementation of the legisla-*
9 *tion referred to in paragraph (2); and*

10 (B) *work with the United States and other*
11 *countries to ensure that such law meets all rel-*
12 *evant international standards.*

Calendar No. 495

115TH CONGRESS
2^D SESSION

H. R. 3776

AN ACT

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

JUNE 28, 2018

Reported with an amendment