



(Original Signature of Member)

117TH CONGRESS
1ST SESSION

H. R. _____

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

IN THE HOUSE OF REPRESENTATIVES

Mr. McCaul 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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Cyber Diplomacy Act of 2021”.

6 (b) TABLE OF CONTENTS.—The table of contents for
7 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 diplomacy.
- Sec. 10. Sense of Congress on cybersecurity sanctions against North Korea and cybersecurity legislation in Vietnam.

1 **SEC. 2. FINDINGS.**

2 Congress makes the following findings:

3 (1) The stated goal of the United States Inter-
4 national Strategy for Cyberspace, launched on May
5 16, 2011, is to “work internationally to promote an
6 open, interoperable, secure, and reliable information
7 and communications infrastructure that supports
8 international trade and commerce, strengthens inter-
9 national security, and fosters free expression and in-
10 novation . . . in which norms of responsible behav-
11 ior guide states’ actions, sustain partnerships, and
12 support the rule of law in cyberspace”.

13 (2) In its June 24, 2013 report, the Group of
14 Governmental Experts on Developments in the Field
15 of Information and Telecommunications in the Con-
16 text of International Security (referred to in this
17 section as “GGE”), established by the United Na-
18 tions General Assembly, concluded that “State sov-
19 ereignty and the international norms and principles
20 that flow from it apply to States’ conduct of [infor-
21 mation and communications technology] ICT-related

1 activities and to their jurisdiction over ICT infra-
2 structure with their territory”.

3 (3) In January 2015, China, Kazakhstan,
4 Kyrgyzstan, Russia, Tajikistan, and Uzbekistan pro-
5 posed a troubling international code of conduct for
6 information security, which could be used as a pre-
7 text for restricting political dissent, and includes
8 “curbing the dissemination of information that in-
9 cites terrorism, separatism or extremism or that in-
10 flames hatred on ethnic, racial or religious grounds”.

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

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

22 (6) At the Antalya Summit on November 15
23 and 16, 2015, the Group of 20 Leaders’
24 communiqué—

1 (A) affirmed the applicability of inter-
2 national law to state behavior in cyberspace;

3 (B) called on states to refrain from cyber-
4 enabled theft of intellectual property for com-
5 mercial gain; and

6 (C) endorsed the view that all states
7 should abide by norms of responsible behavior.

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

13 (8) On December 1, 2016, the Commission on
14 Enhancing National Cybersecurity, which was estab-
15 lished within the Department of Commerce by Exec-
16 utive Order 13718 (81 Fed. Reg. 7441), rec-
17 ommended that “the President should appoint an
18 Ambassador for Cybersecurity to lead U.S. engage-
19 ment with the international community on cyberse-
20 curity strategies, standards, and practices”.

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

1 (A) recognized “the urgent necessity of in-
2 creased international cooperation to promote se-
3 curity and stability in cyberspace”;

4 (B) expressed commitment to “promoting
5 a strategic framework for conflict prevention,
6 cooperation and stability in cyberspace, con-
7 sisting of the recognition of the applicability of
8 existing international law to State behavior in
9 cyberspace, the promotion of voluntary, non-
10 binding norms of responsible State behavior
11 during peacetime, and the development and the
12 implementation of practical cyber confidence
13 building measures (CBMs) between States”;
14 and

15 (C) reaffirmed that “the same rights that
16 people have offline must also be protected on-
17 line”.

18 (10) In testimony before the Select Committee
19 on Intelligence of the Senate on May 11, 2017, Di-
20 rector of National Intelligence Daniel R. Coats iden-
21 tified 6 cyber threat actors, including—

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

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”;

16 (F) criminals, who “are also developing
17 and using sophisticated cyber tools for a variety
18 of purposes including theft, extortion, and fa-
19 cilitation 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
25 lead an interagency effort to develop an engage-

1 ment strategy for international cooperation in
2 cybersecurity; 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 pol-
7 icy 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 vacy 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 com-
17 mittees” means the Committee on Foreign Relations
18 of the Senate and the Committee on Foreign Affairs
19 of the House of Representatives.

20 (2) **INFORMATION AND COMMUNICATIONS**
21 **TECHNOLOGY; ICT.**—The terms “information and
22 communications technology” and “ICT” include
23 hardware, software, and other products or services
24 primarily intended to fulfill or enable the function of
25 information processing and communication by elec-

1 tronic means, including transmission and display, in-
2 cluding via the Internet.

3 (3) EXECUTIVE AGENCY.—The term “Executive
4 agency” has the meaning given the term in section
5 105 of title 5, United States Code.

6 **SEC. 4. UNITED STATES INTERNATIONAL CYBERSPACE**
7 **POLICY.**

8 (a) IN GENERAL.—It is the policy of the United
9 States to work internationally to promote an open, inter-
10 operable, reliable, unfettered, and secure Internet gov-
11 erned by the multi-stakeholder model, which—

12 (1) promotes human rights, democracy, and
13 rule of law, including freedom of expression, innova-
14 tion, communication, and economic prosperity; and

15 (2) respects privacy and guards against decep-
16 tion, fraud, and theft.

17 (b) IMPLEMENTATION.—In implementing the policy
18 described in subsection (a), the President, in consultation
19 with outside actors, including private sector companies,
20 nongovernmental organizations, security researchers, and
21 other relevant stakeholders, in the conduct of bilateral and
22 multilateral relations, shall pursue the following objectives:

23 (1) Clarifying the applicability of international
24 laws and norms to the use of ICT.

1 (2) Reducing and limiting the risk of escalation
2 and retaliation in cyberspace, damage to critical in-
3 frastructure, and other malicious cyber activity that
4 impairs the use and operation of critical infrastruc-
5 ture that provides services to the public.

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

11 (4) Encouraging the responsible development of
12 new, innovative technologies and ICT products that
13 strengthen a secure Internet architecture that is ac-
14 cessible to all.

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
19 knowingly support, cyber-enabled theft of intel-
20 lectual property, including trade secrets or
21 other confidential business information, with
22 the intent of providing competitive advantages
23 to companies or commercial sectors.

24 (B) Countries should take all appropriate
25 and reasonable efforts to keep their territories

1 clear of intentionally wrongful acts using ICTs
2 in violation of international commitments.

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

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

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

1 (F) Countries should not restrict cross-border
2 data flows or require local storage or processing
3 of data.

4 (G) Countries should protect the exercise
5 of human rights and fundamental freedoms on
6 the Internet and commit to the principle that
7 the human rights that people have offline
8 should also be protected online.

9 (6) Advancing, encouraging, and supporting the
10 development and adoption of internationally recognized
11 technical standards and best practices.

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

13 (a) IN GENERAL.—Section 1 of the State Department
14 Basic Authorities Act of 1956 (22 U.S.C. 2651a)
15 is amended—

16 (1) by redesignating subsection (g) as subsection
17 (h); and

18 (2) by inserting after subsection (f) the following
19 new subsection:

20 “(g) BUREAU OF INTERNATIONAL CYBERSPACE POL-
21 ICY.—

22 “(1) IN GENERAL.—There is established, within
23 the Department of State, a Bureau of International
24 Cyberspace Policy (referred to in this subsection as
25 the ‘Bureau’). The head of the Bureau shall have

1 the rank and status of ambassador and shall be ap-
2 pointed by the President, by and with the advice and
3 consent of the Senate.

4 “(2) DUTIES.—

5 “(A) IN GENERAL.—The head of the Bu-
6 reau shall perform such duties and exercise
7 such powers as the Secretary of State shall pre-
8 scribe, including implementing the policy of the
9 United States described in section 4 of the
10 Cyber Diplomacy Act of 2021.

11 “(B) DUTIES DESCRIBED.—The principal
12 duties and responsibilities of the head of the
13 Bureau shall be—

14 “(i) to serve as the principal cyber-
15 space policy official within the senior man-
16 agement of the Department of State and
17 as the advisor to the Secretary of State for
18 cyberspace issues;

19 “(ii) to lead the Department of
20 State’s diplomatic cyberspace efforts, in-
21 cluding efforts relating to international cy-
22 bersecurity, Internet access, Internet free-
23 dom, digital economy, cybercrime, deter-
24 rence and international responses to cyber

1 threats, and other issues that the Sec-
2 retary assigns to the Bureau;

3 “(iii) to promote an open, interoper-
4 able, reliable, unfettered, and secure infor-
5 mation and communications technology in-
6 frastructure globally;

7 “(iv) to represent the Secretary of
8 State in interagency efforts to develop and
9 advance the policy described in section 4 of
10 the Cyber Diplomacy Act of 2021;

11 “(v) to coordinate cyberspace efforts
12 and other relevant functions, including
13 countering terrorists’ use of cyberspace,
14 within the Department of State and with
15 other components of the United States
16 Government;

17 “(vi) to act as a liaison to public and
18 private sector entities on relevant inter-
19 national cyberspace issues;

20 “(vii) to lead United States Govern-
21 ment efforts to establish a global deter-
22 rence framework for malicious cyber activ-
23 ity;

24 “(viii) to develop and execute adver-
25 sary-specific strategies to influence adver-

1 sary decisionmaking through the imposi-
2 tion of costs and deterrence strategies, in
3 coordination with other relevant Executive
4 agencies;

5 “(ix) to advise the Secretary and co-
6 ordinate with foreign governments on ex-
7 ternal responses to national-security-level
8 cyber incidents, including coordination on
9 diplomatic response efforts to support al-
10 lies threatened by malicious cyber activity,
11 in conjunction with members of the North
12 Atlantic Treaty Organization and other
13 like-minded countries;

14 “(x) to promote the adoption of na-
15 tional processes and programs that enable
16 threat detection, prevention, and response
17 to malicious cyber activity emanating from
18 the territory of a foreign country, including
19 as such activity relates to the United
20 States’ European allies, as appropriate;

21 “(xi) to promote the building of for-
22 eign capacity to protect the global network
23 with the goal of enabling like-minded par-
24 ticipation in deterrence frameworks;

1 “(xii) to promote the maintenance of
2 an open and interoperable Internet gov-
3 erned by the multi-stakeholder model, in-
4 stead of by centralized government control;

5 “(xiii) to promote an international
6 regulatory environment for technology in-
7 vestments and the Internet that benefits
8 United States economic and national secu-
9 rity interests;

10 “(xiv) to promote cross-border flow of
11 data and combat international initiatives
12 seeking to impose unreasonable require-
13 ments on United States businesses;

14 “(xv) to promote international policies
15 to protect the integrity of United States
16 and international telecommunications in-
17 frastructure from foreign-based, cyber-en-
18 abled threats;

19 “(xvi) to lead engagement, in coordi-
20 nation with Executive agencies, with for-
21 eign governments on relevant international
22 cyberspace and digital economy issues as
23 described in the Cyber Diplomacy Act of
24 2021;

1 “(xvii) to promote international poli-
2 cies to secure radio frequency spectrum for
3 United States businesses and national se-
4 curity needs;

5 “(xviii) to promote and protect the ex-
6 ercise of human rights, including freedom
7 of speech and religion, through the Inter-
8 net;

9 “(xix) to build capacity of United
10 States diplomatic officials to engage on
11 cyberspace issues;

12 “(xx) to encourage the development
13 and adoption by foreign countries of inter-
14 nationally recognized standards, policies,
15 and best practices; and

16 “(xxi) to consult, as appropriate, with
17 other Executive agencies with related func-
18 tions vested in such Executive agencies by
19 law.

20 “(3) QUALIFICATIONS.—The head of the Bu-
21 reau should be an individual of demonstrated com-
22 petency in the fields of—

23 “(A) cybersecurity and other relevant
24 cyberspace issues; and

25 “(B) international diplomacy.

1 “(4) ORGANIZATIONAL PLACEMENT.—During
2 the 4-year period beginning on the date of the enact-
3 ment of the Cyber Diplomacy Act of 2021, the head
4 of the Bureau shall report to the Under Secretary
5 for Political Affairs or to an official holding a higher
6 position than the Under Secretary for Political Af-
7 fairs in the Department of State. After the conclu-
8 sion of such period, the head of the Bueau shall re-
9 port to an appropriate Under Secretary or to an of-
10 ficial holding a higher position than Under Sec-
11 retary.

12 “(5) RULE OF CONSTRUCTION.—Nothing in
13 this subsection may be construed to preclude the
14 head of the Bureau from being elevated to an Assist-
15 ant Secretary, if such an Assistant Secretary posi-
16 tion does not increase the number of Assistant Sec-
17 retary positions at the Department above the num-
18 ber authorized under subsection (c)(1).”.

19 (b) SENSE OF CONGRESS.—It is the sense of Con-
20 gress that the Bureau of International Cyberspace Policy
21 established under section 1(g) of the State Department
22 Basic Authorities Act of 1956, as added by subsection (a),
23 should have a diverse workforce composed of qualified in-
24 dividuals, including such individuals from traditionally
25 under-represented groups.

1 (c) UNITED NATIONS.—The Permanent Representa-
2 tive of the United States to the United Nations should
3 use the voice, vote, and influence of the United States to
4 oppose any measure that is inconsistent with the policy
5 described in section 4.

6 **SEC. 6. INTERNATIONAL CYBERSPACE EXECUTIVE AR-**
7 **RANGEMENTS.**

8 (a) IN GENERAL.—The President is encouraged to
9 enter into executive arrangements with foreign govern-
10 ments that support the policy described in section 4.

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

13 (1) in subsection (a) by striking “International
14 Relations” and inserting “Foreign Affairs”;

15 (2) in subsection (e)(2)(B), by adding at the
16 end the following new clause:

17 “(iii) A bilateral or multilateral cyberspace
18 agreement.”;

19 (3) by redesignating subsection (f) as sub-
20 section (g); and

21 (4) by inserting after subsection (e) the fol-
22 lowing new subsection:

23 “(f) With respect to any bilateral or multilateral
24 cyberspace agreement under subsection (e)(2)(B)(iii) and
25 the information required to be transmitted to Congress

1 under subsection (a), or with respect to any arrangement
2 that seeks to secure commitments on responsible country
3 behavior in cyberspace consistent with section 4(b)(5) of
4 the Cyber Diplomacy Act of 2021, the Secretary of State
5 shall provide an explanation of such arrangement, includ-
6 ing—

7 “(1) the purpose of such arrangement;

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

10 “(3) how such arrangement will be imple-
11 mented.”.

12 (c) STATUS REPORT.—During the 5-year period im-
13 mediately following the transmittal to Congress of an
14 agreement described in clause (iii) of section
15 112b(e)(2)(B) of title 1, United States Code, as added by
16 subsection (b)(2), or until such agreement has been dis-
17 continued, if discontinued within 5 years, the President
18 shall—

19 (1) notify the appropriate congressional com-
20 mittees if another country fails to adhere to signifi-
21 cant commitments contained in such agreement; and

22 (2) describe the steps that the United States
23 has taken or plans to take to ensure that all such
24 commitments are fulfilled.

1 (d) EXISTING EXECUTIVE ARRANGEMENTS.—Not
2 later than 180 days after the date of the enactment of
3 this Act, the Secretary of State shall brief the appropriate
4 congressional committees regarding any executive bilateral
5 or multilateral cyberspace arrangement in effect before the
6 date of enactment of this Act, including—

7 (1) the arrangement announced between the
8 United States and Japan on April 25, 2014;

9 (2) the arrangement announced between the
10 United States and the United Kingdom on January
11 16, 2015;

12 (3) the arrangement announced between the
13 United States and China on September 25, 2015;

14 (4) the arrangement announced between the
15 United States and Korea on October 16, 2015;

16 (5) the arrangement announced between the
17 United States and Australia on January 19, 2016;

18 (6) the arrangement announced between the
19 United States and India on June 7, 2016;

20 (7) the arrangement announced between the
21 United States and Argentina on April 27, 2017;

22 (8) the arrangement announced between the
23 United States and Kenya on June 22, 2017;

24 (9) the arrangement announced between the
25 United States and Israel on June 26, 2017;

1 (10) the arrangement announced between the
2 United States and France on February 9, 2018;

3 (11) the arrangement announced between the
4 United States and Brazil on May 14, 2018; and

5 (12) any other similar bilateral or multilateral
6 arrangement announced before such date of enact-
7 ment.

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

9 (a) STRATEGY REQUIRED.—Not later than one year
10 after the date of the enactment of this Act, the President,
11 acting through the Secretary of State, and in coordination
12 with the heads of other relevant Federal departments and
13 agencies, shall develop a strategy relating to United States
14 engagement with foreign governments on international
15 norms with respect to responsible state behavior in cyber-
16 space.

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

19 (1) A review of actions and activities under-
20 taken to support the policy described in section 4.

21 (2) A plan of action to guide the diplomacy of
22 the Department of State with regard to foreign
23 countries, including—

24 (A) conducting bilateral and multilateral
25 activities to develop norms of responsible coun-

1 try behavior in cyberspace consistent with the
2 objectives specified in section 4(b)(5); and

3 (B) reviewing the status of existing efforts
4 in relevant multilateral fora, as appropriate, to
5 obtain commitments on international norms in
6 cyberspace.

7 (3) A review of alternative concepts with regard
8 to international norms in cyberspace offered by for-
9 eign countries.

10 (4) A detailed description of new and evolving
11 threats in cyberspace from foreign adversaries, state-
12 sponsored actors, and private actors to—

13 (A) United States national security;

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

16 (C) intellectual property in the United
17 States; and

18 (D) the privacy of citizens of the United
19 States.

20 (5) A review of policy tools available to the
21 President to deter and de-escalate tensions with for-
22 eign countries, state-sponsored actors, and private
23 actors regarding threats in cyberspace, the degree to
24 which such tools have been used, and whether such
25 tools have been effective deterrents.

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

4 (7) A plan of action, developed in consultation
5 with relevant Federal departments and agencies as
6 the President may direct, to guide the diplomacy of
7 the Department of State with regard to inclusion of
8 cyber issues in mutual defense agreements.

9 (c) FORM OF STRATEGY.—

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

14 (2) CLASSIFIED ANNEX.—The strategy required
15 under subsection (a) may include a classified annex,
16 consistent with United States national security inter-
17 ests, if the Secretary of State determines that such
18 annex is appropriate.

19 (d) BRIEFING.—Not later than 30 days after the
20 completion of the strategy required under subsection (a),
21 the Secretary of State shall brief the appropriate congres-
22 sional committees on the strategy, including any material
23 contained in a classified annex.

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

1 process, an individual or group for the nonviolent ex-
2 pression of political, religious, or ideological opinion
3 or belief through the Internet, including electronic
4 mail.

5 “(C) An assessment of the extent to which gov-
6 ernment authorities in the country have sought, in-
7 appropriately and with malicious intent, to collect,
8 request, obtain, or disclose without due process per-
9 sonally identifiable information of a person in con-
10 nection with that person’s nonviolent expression of
11 political, religious, or ideological opinion or belief, in-
12 cluding expression that would be protected by the
13 International Covenant on Civil and Political Rights,
14 adopted at New York December 16, 1966, and en-
15 tered into force March 23, 1976, as interpreted by
16 the United States.

17 “(D) An assessment of the extent to which wire
18 communications and electronic communications are
19 monitored without due process and in contravention
20 to United States policy with respect to the principles
21 of privacy, human rights, democracy, and rule of
22 law.

23 “(2) In compiling data and making assessments
24 under paragraph (1), United States diplomatic personnel
25 should consult with relevant entities, including human

1 rights organizations, the private sector, the governments
2 of like-minded countries, technology and Internet compa-
3 nies, and other appropriate nongovernmental organiza-
4 tions or entities.

5 “(3) In this subsection—

6 “(A) the term ‘electronic communication’ has
7 the meaning given the term in section 2510 of title
8 18, United States Code;

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

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

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

18 (2) in section 502B (22 U.S.C. 2304)—

19 (A) by redesignating the second subsection
20 (i) (relating to child marriage) as subsection (j);
21 and

22 (B) by adding at the end the following new
23 subsection:

24 “(h)(1) The report required under subsection (b)
25 shall include an assessment of freedom of expression with

1 respect to electronic information in each foreign country,
2 which information shall include the following:

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

11 “(B) An assessment of the extent to which gov-
12 ernment authorities in the country have persecuted
13 or otherwise punished, arbitrarily and without due
14 process, an individual or group for the nonviolent ex-
15 pression of political, religious, or ideological opinion
16 or belief through the Internet, including electronic
17 mail.

18 “(C) An assessment of the extent to which gov-
19 ernment authorities in the country have sought, in-
20 appropriately and with malicious intent, to collect,
21 request, obtain, or disclose without due process per-
22 sonally identifiable information of a person in con-
23 nection with that person’s nonviolent expression of
24 political, religious, or ideological opinion or belief, in-
25 cluding expression that would be protected by the

1 International Covenant on Civil and Political Rights,
2 adopted at New York December 16, 1966, and en-
3 tered into force March 23, 1976, as interpreted by
4 the United States.

5 “(D) An assessment of the extent to which wire
6 communications and electronic communications are
7 monitored without due process and in contravention
8 to United States policy with respect to the principles
9 of privacy, human rights, democracy, and rule of
10 law.

11 “(2) In compiling data and making assessments
12 under paragraph (1), United States diplomatic personnel
13 should consult with relevant entities, including human
14 rights organizations, the private sector, the governments
15 of like-minded countries, technology and Internet compa-
16 nies, and other appropriate nongovernmental organiza-
17 tions or entities.

18 “(3) In this subsection—

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

22 “(B) the term ‘Internet’ has the meaning given
23 the term in section 231(e)(3) of the Communications
24 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 the term in section 2510 of title 18,
6 United States Code.”.

7 **SEC. 9. GAO REPORT ON CYBER DIPLOMACY.**

8 Not later than one year after the date of the enact-
9 ment of this Act, the Comptroller General of the United
10 States shall submit a report and provide a briefing to the
11 appropriate congressional committees that includes—

12 (1) an assessment of the extent to which United
13 States diplomatic processes and other efforts with
14 foreign countries, including through multilateral
15 fora, bilateral engagements, and negotiated cyber-
16 space agreements, advance the full range of United
17 States interests in cyberspace, including the policy
18 described in section 4;

19 (2) an assessment of the Department of State’s
20 organizational structure and approach to managing
21 its diplomatic efforts to advance the full range of
22 United States interests in cyberspace, including a re-
23 view of—

1 (A) the establishment of a bureau in the
2 Department of State to lead the Department's
3 international cyber mission;

4 (B) the current or proposed diplomatic
5 mission, structure, staffing, funding, and activi-
6 ties of the bureau;

7 (C) how the establishment of the bureau
8 has impacted or is likely to impact the structure
9 and organization of the Department; and

10 (D) what challenges, if any, the Depart-
11 ment has faced or will face in establishing such
12 bureau; and

13 (3) any other matters determined relevant by
14 the Comptroller General.

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

18 It is the sense of Congress that—

19 (1) the President should designate all entities
20 that knowingly engage in significant activities under-
21 mining cybersecurity through the use of computer
22 networks or systems against foreign persons, govern-
23 ments, or other entities on behalf of the Government
24 of North Korea, consistent with section 209(b) of

1 the North Korea Sanctions and Policy Enhancement
2 Act of 2016 (22 U.S.C. 9229(b));

3 (2) the cybersecurity law approved by the Na-
4 tional Assembly of Vietnam on June 12, 2018—

5 (A) may not be consistent with inter-
6 national trade standards; and

7 (B) may endanger the privacy of citizens
8 of Vietnam; and

9 (3) the Government of Vietnam should work
10 with the United States and other countries to ensure
11 that such law meets all relevant international stand-
12 ards.