

**MARKUP of H. Res. 75, H.R. 739,  
H. Res. 156, H.R. 596, and H.R. 295**

---

---

**MARKUP**  
BEFORE THE  
**COMMITTEE ON FOREIGN AFFAIRS**  
**HOUSE OF REPRESENTATIVES**

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

—————  
MARCH 7, 2019  
—————

**Serial No. 116–11**

Printed for the use of the Committee on Foreign Affairs



Available: <http://www.foreignaffairs.house.gov/>, <http://docs.house.gov/>,  
or <http://www.govinfo.gov>

—————  
U.S. GOVERNMENT PUBLISHING OFFICE

35–369PDF

WASHINGTON : 2019

COMMITTEE ON FOREIGN AFFAIRS

ELIOT L. ENGEL, New York, *Chairman*

BRAD SHERMAN, California	MICHAEL T. McCAUL, Texas, <i>Ranking Member</i>
GREGORY W. MEEKS, New York	CHRISTOPHER H. SMITH, New Jersey
ALBIO SIRES, New Jersey	STEVE CHABOT, Ohio
GERALD E. CONNOLLY, Virginia	JOE WILSON, South Carolina
THEODORE E. DEUTCH, Florida	SCOTT PERRY, Pennsylvania
KAREN BASS, California	TED S. YOHO, Florida
WILLIAM KEATING, Massachusetts	ADAM KINZINGER, Illinois
DAVID CICILLINE, Rhode Island	LEE ZELDIN, New York
AMI BERA, California	JIM SENSENBRENNER, Wisconsin
JOAQUIN CASTRO, Texas	ANN WAGNER, Missouri
DINA TITUS, Nevada	BRIAN MAST, Florida
ADRIANO ESPAILLAT, New York	FRANCIS ROONEY, Florida
TED LIEU, California	BRIAN FITZPATRICK, Pennsylvania
SUSAN WILD, Pennsylvania	JOHN CURTIS, Utah
DEAN PHILLIPS, Minnesota	KEN BUCK, Colorado
ILHAN OMAR, Minnesota	RON WRIGHT, Texas
COLIN ALLRED, Texas	GUY RESCHENTHALER, Pennsylvania
ANDY LEVIN, Michigan	TIM BURCHETT, Tennessee
ABIGAIL SPANBERGER, Virginia	GREG PENCE, Indiana
CHRISSE HOULAHAN, Pennsylvania	STEVE WATKINS, Kansas
TOM MALINOWSKI, New Jersey	MIKE GUEST, Mississippi
DAVID TRONE, Maryland	
JIM COSTA, California	
JUAN VARGAS, California	
VICENTE GONZALEZ, Texas	

JASON STEINBAUM, *Staff Director*

BRENDAN SHIELDS, *Republican Staff Director*

# CONTENTS

	Page
APPENDIX	
Hearing Notice .....	106
Hearing Minutes .....	107
Hearing Attendance .....	108
Prepared statement submitted from Representative Castro .....	109
MARKUP SUMMARY	
Markup Summary .....	111
ADDITIONAL MATERIALS SUBMITTED FOR THE RECORD	
H. Res. 75, Strongly Condemning the January 2019 Terrorist attack on the 14 Riverside Complex in Nairobi, Kenya .....	2
H.R. 739, the Cyber Diplomacy Act of 2019 With the McCaul Amendment .....	6
Amendment in the Nature of a Substitute to H.R. 739 Offered by Mr. McCaul of Texas .....	35
H. Res. 156 Calling for Accountability and Justice for the Assassination of Boris Nemtsov with the two Malinowski Amendments .....	64
Amendment to H. Res. 156 Offered by Mr. Malinowski of New Jersey (1 of 2 Listed) .....	72
Amendment to H. Res. 156 Offered by Mr. Malinowski of New Jersey (2 of 2 Listed) .....	73
H.R. 596, Crimea Annexation Nonrecognition Act with the Connolly Amend- ment in the Nature of a Substitute .....	74
Amendment in the Nature of a Substitute to H.R. 596 Offered by Mr. Con- nolly of Virginia .....	76
H.R. 295, End Banking for Human Traffickers Act of 2019 with the Engel Amendment in the Nature of a Substitute .....	78
Amendment in the Nature of a Substitute to H.R. 295 Offered by Mr. Engel of New York .....	87



## **MARKUP OF VARIOUS MEASURES**

**Thursday, March 7, 2019**

HOUSE OF REPRESENTATIVES  
COMMITTEE ON FOREIGN AFFAIRS  
*Washington, DC*

The committee met, pursuant to notice, at 10:05 a.m., in Room 2172 Rayburn House Office Building, Hon. Eliot Engel (chairman of the committee) presiding.

Chairman ENGEL. So pursuant to notice, we meet today to mark-up five bipartisan measures. Without objection, all members may have 5 days to submit statements or extraneous materials on today's business.

As members were notified yesterday, we intend to consider today's measures en bloc. The measures are H. Res. 75, strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya; H.R. 739, the Cyber Diplomacy Act of 2019 with the McCaul Amendment; H. Res. 156 calling for accountability and justice for the assassination of Boris Nemtsov with the two Malinowski Amendments; H.R. 596, Crimea Annexation Non-recognition Act with the Connolly Amendment in the nature of a substitute; and H.R. 295, End Banking for Human Traffickers Act of 2019 with the Engel Amendment in the nature of a substitute.

[The bills and resolutions offered en bloc follow:]



116TH CONGRESS  
1ST SESSION

# H. RES. 75

Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya, offering condolences to the family and friends of the victims, and reaffirming solidarity with the people of Kenya.

---

## IN THE HOUSE OF REPRESENTATIVES

JANUARY 24, 2019

Mr. ENGEL (for himself, Mr. McCAUL, Ms. BASS, and Mr. SMITH of New Jersey) submitted the following resolution; which was referred to the Committee on Foreign Affairs

---

## RESOLUTION

Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya, offering condolences to the family and friends of the victims, and reaffirming solidarity with the people of Kenya.

Whereas, on January 15, 2019, armed gunmen attacked the 14 Riverside Complex in Nairobi, Kenya, killing at least 21 people during the 20-hour siege;

Whereas one of the individuals killed in this heinous act of violence was an American citizen named Jason Spindler, a 9/11 survivor and former Peace Corps volunteer who was the CEO and managing director of a strategy and investment firm in Nairobi;

Whereas Kenyan security forces rescued more than 700 civilians from the complex;

Whereas al-Shabaab, an al-Qaeda affiliated terrorist organization based in Somalia designated as a foreign terrorist organization by the Department of State, has claimed responsibility for the attack on the 14 Riverside Complex;

Whereas Kenya has previously been a target for al-Qaeda affiliated terrorist attacks in August 1998, when the United States embassy in Nairobi, Kenya, and the United States embassy in Dar es Salaam, Tanzania, were simultaneously bombed, killing 224 people and injuring over 5,000 people;

Whereas al-Shabaab has previously perpetrated numerous mass-casualty terrorist attacks in Kenya, notably the siege at the Westgate Mall in Nairobi in September 2013, which killed 67 people, and the assault on Garissa University College in April 2015, which killed 148 people;

Whereas the United States and Kenya share a longstanding and mutually beneficial political, economic, and security partnership; and

Whereas security cooperation between the United States and Kenya plays an essential role in combating terrorism and violent extremism in the Horn of Africa, particularly efforts to combat al-Shabaab; Now, therefore, be it

1       *Resolved*, That the House of Representatives—

2               (1) condemns in the strongest terms the recent  
3       terrorist attack by al-Shabaab in Nairobi, Kenya,  
4       that resulted in the tragic loss of 21 lives;

5               (2) offers its deepest condolences to the family  
6       and friends of the victims and to the Republic of

1 Kenya, and reaffirms its solidarity with the Kenyan  
2 people;

3 (3) honors the memory of Jason Spindler, who  
4 was murdered in this horrific terrorist attack;

5 (4) recognizes the heroism exhibited by Kenyan  
6 citizens, first responders, security forces, and the  
7 Kenya Red Cross Society to rescue those held hos-  
8 tage during the siege;

9 (5) expresses its support for the Government of  
10 Kenya's efforts to combat terrorism and violent ex-  
11 tremism, including efforts to prevent, detect, and  
12 deter future attacks, and encourages all Kenyans to  
13 stand together in condemning terrorism and violent  
14 extremism;

15 (6) recognizes Kenya's contributions to coun-  
16 tering terrorism and violent extremism in the region,  
17 particularly al-Shabaab, including as troop contribu-  
18 tors to the African Union Mission in Somalia;

19 (7) recognizes the important role of United  
20 States assistance to combat al-Shabaab and other  
21 terrorist activity in the region, including efforts to  
22 build Kenya's capacity to respond to and prevent  
23 such attacks; and

24 (8) urges the Government of Kenya to work ex-  
25 pediently to bring the perpetrators to justice, ad-



5

4

1 hering to the rule of law, respect for human rights,  
2 and due process in its efforts to counter terrorism  
3 and violent extremism.

○



116TH CONGRESS  
1ST SESSION

# H. R. 739

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

---

## IN THE HOUSE OF REPRESENTATIVES

JANUARY 24, 2019

Mr. MCCAUL (for himself and Mr. ENGEL) introduced the following bill; which was referred to the Committee on Foreign Affairs

---

## 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 2019”.

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 threats and data misuse.  
Sec. 10. Sense of Congress on cybersecurity sanctions against North Korea and  
cybersecurity legislation in Vietnam.  
Sec. 11. Rule of construction.

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  
22 activities and to their jurisdiction over ICT infra-  
23 structure with their territory”.

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

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

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

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

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

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

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

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

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

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

22 (A) recognized “the urgent necessity of in-  
23 creased international cooperation to promote se-  
24 curity and stability in cyberspace”;

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

12 (C) reaffirmed that “the same rights that  
13 people have offline must also be protected on-  
14 line”.

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

19 (A) Russia, for “efforts to influence the  
20 2016 US election”;

21 (B) China, for “actively targeting the US  
22 Government, its allies, and US companies for  
23 cyber espionage”;

24 (C) Iran, for “leverag[ing] cyber espionage,  
25 propaganda, and attacks to support its security

1 priorities, influence events and foreign percep-  
2 tions, and counter threats”;

3 (D) North Korea, for “previously  
4 conduct[ing] cyber-attacks against US commer-  
5 cial entities—specifically, Sony Pictures Enter-  
6 tainment in 2014”;

7 (E) terrorists, who “use the Internet to or-  
8 ganize, recruit, spread propaganda, raise funds,  
9 collect intelligence, inspire action by followers,  
10 and coordinate operations”; and

11 (F) criminals, who “are also developing  
12 and using sophisticated cyber tools for a variety  
13 of purposes including theft, extortion, and fa-  
14 cilitation of other criminal activities”.

15 (11) On May 11, 2017, President Donald J.  
16 Trump issued Executive Order 13800 (82 Fed. Reg.  
17 22391), entitled “Strengthening the Cybersecurity of  
18 Federal Networks and Infrastructure”, which—

19 (A) designates the Secretary of State to  
20 lead an interagency effort to develop an engage-  
21 ment strategy for international cooperation in  
22 cybersecurity; and

23 (B) notes that “the United States is espe-  
24 cially dependent on a globally secure and resil-  
25 ient internet and must work with allies and

1 other partners toward maintaining . . . the pol-  
2 icy of the executive branch to promote an open,  
3 interoperable, reliable, and secure internet that  
4 fosters efficiency, innovation, communication,  
5 and economic prosperity, while respecting pri-  
6 vacy and guarding against disruption, fraud,  
7 and theft”.

8 **SEC. 3. DEFINITIONS.**

9 In this Act:

10 (1) **APPROPRIATE CONGRESSIONAL COMMIT-**  
11 **TEES.**—The term “appropriate congressional com-  
12 mittees” means the Committee on Foreign Relations  
13 of the Senate and the Committee on Foreign Affairs  
14 of the House of Representatives.

15 (2) **INFORMATION AND COMMUNICATIONS**  
16 **TECHNOLOGY; ICT.**—The terms “information and  
17 communications technology” and “ICT” include  
18 hardware, software, and other products or services  
19 primarily intended to fulfill or enable the function of  
20 information processing and communication by elec-  
21 tronic means, including transmission and display, in-  
22 cluding via the Internet.

23 (3) **EXECUTIVE AGENCY.**—The term “Executive  
24 agency” has the meaning given the term in section  
25 105 of title 5, United States Code.



1 **SEC. 4. UNITED STATES INTERNATIONAL CYBERSPACE**

2 **POLICY.**

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

7 (1) promotes human rights, democracy, and  
8 rule of law, including freedom of expression, innova-  
9 tion, communication, and economic prosperity; and

10 (2) respects privacy and guards against decep-  
11 tion, fraud, and theft.

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

18 (1) Clarifying the applicability of international  
19 laws and norms to the use of ICT.

20 (2) Reducing and limiting the risk of escalation  
21 and retaliation in cyberspace, damage to critical in-  
22 frastructure, and other malicious cyber activity that  
23 impairs the use and operation of critical infrastruc-  
24 ture that provides services to the public.

25 (3) Cooperating with like-minded democratic  
26 countries that share common values and cyberspace

1 policies with the United States, including respect for  
2 human rights, democracy, and the rule of law, to ad-  
3 vance such values and policies internationally.

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

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

11 (A) Countries should not conduct, or  
12 knowingly support, cyber-enabled theft of intel-  
13 lectual property, including trade secrets or  
14 other confidential business information, with  
15 the intent of providing competitive advantages  
16 to companies or commercial sectors.

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

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

1 and should take appropriate measures to pro-  
2 tect their critical infrastructure from ICT  
3 threats.

4 (D) 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 (also known as “computer  
9 emergency response teams” or “cybersecurity  
10 incident response teams”) of another country or  
11 authorize emergency response teams to engage  
12 in malicious international activity.

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

18 (F) Countries should not restrict cross-bor-  
19 der data flows or require local storage or pro-  
20 cessing of data.

21 (G) Countries should protect the exercise  
22 of human rights and fundamental freedoms on  
23 the Internet and commit to the principle that  
24 the human rights that people have offline  
25 should also be protected online.

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

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

5           (a) IN GENERAL.—Section 1 of the State Depart-  
6           ment Basic Authorities Act of 1956 (22 U.S.C. 2651a)  
7           is amended—

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

10           (2) by inserting after subsection (f) the fol-  
11           lowing:

12           “(g) OFFICE OF INTERNATIONAL CYBERSPACE POL-  
13           ICY.—

14           “(1) IN GENERAL.—There is established, within  
15           the Department of State, an Office of International  
16           Cyberspace Policy (referred to in this subsection as  
17           the ‘Office’). The head of the Office shall have the  
18           rank and status of ambassador and shall be ap-  
19           pointed by the President, by and with the advice and  
20           consent 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 4 of the Cyber Di-  
2 plomacy Act of 2019.

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

6 “(i) to serve as the principal cyber-  
7 space policy official within the senior man-  
8 agement of the Department of State and  
9 as the advisor to the Secretary of State for  
10 cyberspace issues;

11 “(ii) to lead the Department of  
12 State’s diplomatic cyberspace efforts, in-  
13 cluding efforts relating to international cy-  
14 bersecurity, Internet access, Internet free-  
15 dom, digital economy, cybercrime, deter-  
16 rence and international responses to cyber  
17 threats, and other issues that the Sec-  
18 retary assigns to the Office;

19 “(iii) to promote an open, interoper-  
20 able, reliable, unfettered, and secure infor-  
21 mation and communications technology in-  
22 frastructure globally;

23 “(iv) to represent the Secretary of  
24 State in interagency efforts to develop and

1 advance the policy described in section 4 of  
2 the Cyber Diplomacy Act of 2019;

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

9 “(vi) to act as a liaison to public and  
10 private sector entities on relevant inter-  
11 national cyberspace issues;

12 “(vii) to lead United States Govern-  
13 ment efforts to establish a global deter-  
14 rence framework for malicious cyber activ-  
15 ity;

16 “(viii) to develop and execute adver-  
17 sary-specific strategies to influence adver-  
18 sary decisionmaking through the imposi-  
19 tion of costs and deterrence strategies, in  
20 coordination with other relevant Executive  
21 agencies;

22 “(ix) to advise the Secretary and co-  
23 ordinate with foreign governments on ex-  
24 ternal responses to national-security-level  
25 cyber incidents, including coordination on

1 diplomatic response efforts to support al-  
2 lies threatened by malicious cyber activity,  
3 in conjunction with members of the North  
4 Atlantic Treaty Organization and other  
5 like-minded countries;

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

13 “(xi) to promote the building of for-  
14 eign capacity to protect the global network  
15 with the goal of enabling like-minded par-  
16 ticipation in deterrence frameworks;

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

21 “(xiii) to promote an international  
22 regulatory environment for technology in-  
23 vestments and the Internet that benefits  
24 United States economic and national secu-  
25 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  
7 and international telecommunications in-  
8 frastructure from foreign-based, cyber-en-  
9 abled threats;

10          “(xvi) to lead engagement, in coordi-  
11 nation with Executive agencies, with for-  
12 eign governments on cyberspace and digital  
13 economy issues as described in the Cyber  
14 Diplomacy Act of 2019;

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

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

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



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

5           “(xxi) to consult, as appropriate, with  
6           other Executive agencies with related func-  
7           tions vested in such Executive agencies by  
8           law.

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

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

14                 “(B) international diplomacy.

15          “(4) ORGANIZATIONAL PLACEMENT.—During  
16          the 4-year period beginning on the date of the enact-  
17          ment of the Cyber Diplomacy Act of 2019, the head  
18          of the Office shall report to the Under Secretary for  
19          Political Affairs or to an official holding a higher po-  
20          sition than the Under Secretary for Political Affairs  
21          in the Department of State. After the conclusion of  
22          such period, the head of the Office shall report to  
23          an appropriate Under Secretary or to an official  
24          holding a higher position than Under Secretary.

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

3                   “(A) the Office from being elevated to a  
4 Bureau within the Department of State; or

5                   “(B) the head of the Office from being ele-  
6 vated to an Assistant Secretary, if such an As-  
7 sistant Secretary position does not increase the  
8 number of Assistant Secretary positions at the  
9 Department above the number authorized under  
10 subsection (e)(1).”.

11           (b) SENSE OF CONGRESS.—It is the sense of Con-  
12 gress that the Office of International Cyberspace Policy  
13 established under section 1(g) of the State Department  
14 Basic Authorities Act of 1956, as added by subsection (a),  
15 should be a Bureau of the Department of State and the  
16 head of such Office should report directly to the Secretary  
17 of State or Deputy Secretary of State.

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

1 **SEC. 6. INTERNATIONAL CYBERSPACE EXECUTIVE AR-**  
2 **RANGEMENTS.**

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

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

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

10 (2) in subsection (e)(2)(B), by adding at the  
11 end the following:

12 “(iii) A bilateral or multilateral cyberspace  
13 agreement.”;

14 (3) by redesignating subsection (f) as sub-  
15 section (g); and

16 (4) by inserting after subsection (e) the fol-  
17 lowing:

18 “(f) With respect to any bilateral or multilateral  
19 cyberspace agreement under subsection (e)(2)(B)(iii) and  
20 the information required to be transmitted to Congress  
21 under subsection (a), or with respect to any arrangement  
22 that seeks to secure commitments on responsible country  
23 behavior in cyberspace consistent with section 4(b)(5) of  
24 the Cyber Diplomacy Act of 2019, the Secretary of State  
25 shall provide an explanation of such arrangement, includ-  
26 ing—

1 “(1) the purpose of such arrangement;

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

4 “(3) how such arrangement will be imple-  
5 mented.”.

6 (c) STATUS REPORT.—During the 5-year period im-  
7 mediately following the transmittal to Congress of an  
8 agreement described in section 112b(e)(2)(B)(iii) of title  
9 1, United States Code, as added by subsection (b)(2), or  
10 until such agreement has been discontinued, if discon-  
11 tinued within 5 years, the President shall—

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

15 (2) describe the steps that the United States  
16 has taken or plans to take to ensure that all such  
17 commitments are fulfilled.

18 (d) EXISTING EXECUTIVE ARRANGEMENTS.—Not  
19 later than 180 days after the date of the enactment of  
20 this Act, the Secretary of State shall brief the appropriate  
21 congressional committees regarding any executive bilateral  
22 or multilateral cyberspace arrangement in effect before the  
23 date of enactment of this Act, including—

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

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

22          (12) any other similar bilateral or multilateral  
23 arrangement announced before such date of enact-  
24 ment.

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

2 (a) STRATEGY REQUIRED.—Not later than 1 year  
3 after the date of the enactment of this Act, the President,  
4 acting through the Secretary of State, and in coordination  
5 with the heads of other relevant Federal departments and  
6 agencies, shall develop a strategy relating to United States  
7 engagement with foreign governments on international  
8 norms with respect to responsible state behavior in cyber-  
9 space.

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

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

14 (2) A plan of action to guide the diplomacy of  
15 the Department of State with regard to foreign  
16 countries, including—

17 (A) conducting bilateral and multilateral  
18 activities to develop norms of responsible coun-  
19 try behavior in cyberspace consistent with the  
20 objectives under section 4(b)(5); and

21 (B) reviewing the status of existing efforts  
22 in relevant multilateral fora, as appropriate, to  
23 obtain commitments on international norms in  
24 cyberspace.

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

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

7                   (A) United States national security;

8                   (B) Federal and private sector cyberspace  
9 infrastructure of the United States;

10                  (C) intellectual property in the United  
11 States; and

12                  (D) the privacy of citizens of the United  
13 States.

14           (5) A review of policy tools available to the  
15 President to deter and de-escalate tensions with for-  
16 eign countries, state-sponsored actors, and private  
17 actors regarding threats in cyberspace, the degree to  
18 which such tools have been used, and whether such  
19 tools have been effective deterrents.

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

23           (7) A plan of action, developed in consultation  
24 with relevant Federal departments and agencies as  
25 the President may direct, to guide the diplomacy of

1 the Department of State with regard to inclusion of  
2 cyber issues in mutual defense agreements.

3 (c) FORM OF STRATEGY.—

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

8 (2) CLASSIFIED ANNEX.—The strategy required  
9 under subsection (a) may include a classified annex,  
10 consistent with United States national security inter-  
11 ests, if the Secretary of State determines that such  
12 annex is appropriate.

13 (d) BRIEFING.—Not later than 30 days after the  
14 completion of the strategy required under subsection (a),  
15 the Secretary of State shall brief the appropriate congres-  
16 sional committees on the strategy, including any material  
17 contained in a classified annex.

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

20 (1) not later than 90 days after any material  
21 change to United States policy described in such  
22 strategy; and

23 (2) not later than 1 year after the inauguration  
24 of each new President.



1 (f) PREEXISTING REQUIREMENT.—The Rec-  
2 ommendations to the President on Protecting American  
3 Cyber Interests through International Engagement, pre-  
4 pared by the Office of the Coordinator for Cyber Issues  
5 on May 31, 2018, pursuant to section 3(e) of Executive  
6 Order 13800 (82 Fed. Reg. 22391), shall be deemed to  
7 satisfy the requirement under subsection (a).

8 **SEC. 8. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS**  
9 **PRACTICES.**

10 Section 116 of the Foreign Assistance Act of 1961  
11 (22 U.S.C. 2151n) is amended by adding at the end the  
12 following:

13 “(h)(1) The report required under subsection (d)  
14 shall include an assessment of freedom of expression with  
15 respect to electronic information in each foreign country  
16 that includes the following:

17 “(A) An assessment of the extent to which gov-  
18 ernment authorities in the country inappropriately  
19 attempt to filter, censor, or otherwise block or re-  
20 move nonviolent expression of political or religious  
21 opinion or belief through the Internet, including  
22 electronic mail, and a description of the means by  
23 which such authorities attempt to inappropriately  
24 block or remove such expression.

1           “(B) An assessment of the extent to which gov-  
2           ernment authorities in the country have persecuted  
3           or otherwise punished, arbitrarily and without due  
4           process, an individual or group for the nonviolent ex-  
5           pression of political, religious, or ideological opinion  
6           or belief through the Internet, including electronic  
7           mail.

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

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

1 “(2) In compiling data and making assessments  
2 under paragraph (1), United States diplomatic personnel  
3 should consult with relevant entities, including human  
4 rights organizations, the private sector, the governments  
5 of like-minded countries, technology and Internet compa-  
6 nies, and other appropriate nongovernmental organiza-  
7 tions or entities.

8 “(3) In this subsection—

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

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

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

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

21 **SEC. 9. GAO REPORT ON CYBER THREATS AND DATA MIS-**  
22 **USE.**

23 Not later than 1 year after the date of the enactment  
24 of this Act, the Comptroller General of the United States

1 shall submit a report and provide a briefing to the appro-  
2 priate congressional committees that includes—

3 (1) a description of the primary threats to the  
4 personal information of United States citizens from  
5 international actors within the cyberspace domain;

6 (2) an assessment of the extent to which United  
7 States diplomatic processes and other efforts with  
8 foreign countries, including through multilateral  
9 fora, bilateral engagements, and negotiated cyber-  
10 space agreements, strengthen the protections of  
11 United States citizens' personal information;

12 (3) an assessment of the Department of State's  
13 report in response to Executive Order 13800 (82  
14 Fed. Reg. 22391), which documents an engagement  
15 strategy for international cooperation in cybersecu-  
16 rity and the extent to which this strategy addresses  
17 protections of United States citizens' personal infor-  
18 mation;

19 (4) recommendations for United States policy-  
20 makers on methods to properly address and  
21 strengthen the protections of United States citizens'  
22 personal information from misuse by international  
23 actors; and

24 (5) any other matters deemed relevant by the  
25 Comptroller General.

1 **SEC. 10. SENSE OF CONGRESS ON CYBERSECURITY SANC-**  
2 **TIONS AGAINST NORTH KOREA AND CYBER-**  
3 **SECURITY LEGISLATION IN VIETNAM.**

4 It is the sense of Congress that—

5 (1) the President should designate all entities  
6 that knowingly engage in significant activities under-  
7 mining cybersecurity through the use of computer  
8 networks or systems against foreign persons, govern-  
9 ments, or other entities on behalf of the Government  
10 of North Korea, consistent with section 209(b) of  
11 the North Korea Sanctions and Policy Enhancement  
12 Act of 2016 (22 U.S.C. 9229(b));

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

15 (A) may not be consistent with inter-  
16 national trade standards; and

17 (B) may endanger the privacy of citizens  
18 of Vietnam; and

19 (3) the Government of Vietnam should work  
20 with the United States and other countries to ensure  
21 that such law meets all relevant international stand-  
22 ards.

23 **SEC. 11. RULE OF CONSTRUCTION.**

24 (a) **RULE OF CONSTRUCTION.**—Nothing in this Act  
25 may be construed to infringe upon the related functions

34

29

1 of any Executive agency vested in such agency under any  
2 provision of law.

○

G:\M16\MCCAUL\MCCAUL\_014.XML

**AMENDMENT IN THE NATURE OF A SUBSTITUTE  
TO H.R. 739  
OFFERED BY MR. MCCAUL OF TEXAS**

Strike all after the enacting clause and insert the following:

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

2 (a) SHORT TITLE.—This Act may be cited as the  
3 “Cyber Diplomacy Act of 2019”.

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 diplomacy.
- Sec. 10. Sense of Congress on cybersecurity sanctions against North Korea and  
cybersecurity legislation in Vietnam.
- Sec. 11. Rule of construction.

**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

1 international trade and commerce, strengthens inter-  
2 national security, and fosters free expression and in-  
3 novation . . . in which norms of responsible behav-  
4 ior guide states' actions, sustain partnerships, and  
5 support the rule of law in cyberspace”.

6 (2) In its June 24, 2013 report, the Group of  
7 Governmental Experts on Developments in the Field  
8 of Information and Telecommunications in the Con-  
9 text of International Security (referred to in this  
10 section as “GGE”), established by the United Na-  
11 tions General Assembly, concluded that “State sov-  
12 ereignty and the international norms and principles  
13 that flow from it apply to States’ conduct of [infor-  
14 mation and communications technology] ICT-related  
15 activities and to their jurisdiction over ICT infra-  
16 structure with their territory”.

17 (3) In January 2015, China, Kazakhstan,  
18 Kyrgyzstan, Russia, Tajikistan, and Uzbekistan pro-  
19 posed a troubling international code of conduct for  
20 information security, which could be used as a pre-  
21 text for restricting political dissent, and includes  
22 “curbing the dissemination of information that in-  
23 cites terrorism, separatism or extremism or that in-  
24 flames hatred on ethnic, racial or religious grounds”.



G:\M\16\MCCAUL\MCCAUL\_014.XML

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

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

12 (6) At the Antalya Summit on November 15  
13 and 16, 2015, the Group of 20 Leaders’  
14 communiqué—

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

17 (B) called on states to refrain from cyber-  
18 enabled theft of intellectual property for com-  
19 mercial gain; and

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

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

G:\M16\MCCAUL\MCCAUL\_014.XML

4

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, which was estab-  
5       lished within the Department of Commerce by Exec-  
6       utive Order 13718 (81 Fed. Reg. 7441), rec-  
7       ommended that “the President should appoint an  
8       Ambassador for Cybersecurity to lead U.S. engage-  
9       ment with the international community on cyberse-  
10      curity strategies, standards, and practices”.

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

14           (A) recognized “the urgent necessity of in-  
15      creased international cooperation to promote se-  
16      curity and stability in cyberspace”;

17           (B) expressed commitment to “promoting  
18      a strategic framework for conflict prevention,  
19      cooperation and stability in cyberspace, con-  
20      sisting of the recognition of the applicability of  
21      existing international law to State behavior in  
22      cyberspace, the promotion of voluntary, non-  
23      binding norms of responsible State behavior  
24      during peacetime, and the development and the  
25      implementation of practical cyber confidence

1 building measures (CBMs) between States”;  
2 and

3 (C) reaffirmed that “the same rights that  
4 people have offline must also be protected on-  
5 line”.

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

10 (A) Russia, for “efforts to influence the  
11 2016 US election”;

12 (B) China, for “actively targeting the US  
13 Government, its allies, and US companies for  
14 cyber espionage”;

15 (C) Iran, for “leverag[ing] cyber espionage,  
16 propaganda, and attacks to support its security  
17 priorities, influence events and foreign percep-  
18 tions, and counter threats”;

19 (D) North Korea, for “previously  
20 conduct[ing] cyber-attacks against US commer-  
21 cial entities—specifically, Sony Pictures Enter-  
22 tainment in 2014”;

23 (E) terrorists, who “use the Internet to or-  
24 ganize, recruit, spread propaganda, raise funds,

G:\M\16\MCCAUL\MCCAUL\_014.XML

6

1 collect intelligence, inspire action by followers,  
2 and coordinate operations”; and

3 (F) criminals, who “are also developing  
4 and using sophisticated cyber tools for a variety  
5 of purposes including theft, extortion, and fa-  
6 cilitation of other criminal activities”.

7 (11) On May 11, 2017, President Donald J.  
8 Trump issued Executive Order 13800 (82 Fed. Reg.  
9 22391), entitled “Strengthening the Cybersecurity of  
10 Federal Networks and Infrastructure”, which—

11 (A) designates the Secretary of State to  
12 lead an interagency effort to develop an engage-  
13 ment strategy for international cooperation in  
14 cybersecurity; and

15 (B) notes that “the United States is espe-  
16 cially dependent on a globally secure and resil-  
17 ient internet and must work with allies and  
18 other partners toward maintaining . . . the pol-  
19 icy of the executive branch to promote an open,  
20 interoperable, reliable, and secure internet that  
21 fosters efficiency, innovation, communication,  
22 and economic prosperity, while respecting pri-  
23 vacy and guarding against disruption, fraud,  
24 and theft”.

1 **SEC. 3. DEFINITIONS.**

2 In this Act:

3 (1) **APPROPRIATE CONGRESSIONAL COMMIT-**  
4 **TEES.**—The term “appropriate congressional com-

5 mittees” means the Committee on Foreign Relations  
6 of the Senate and the Committee on Foreign Affairs  
7 of the House of Representatives.

8 (2) **INFORMATION AND COMMUNICATIONS**  
9 **TECHNOLOGY; ICT.**—The terms “information and  
10 communications technology” and “ICT” include  
11 hardware, software, and other products or services  
12 primarily intended to fulfill or enable the function of  
13 information processing and communication by elec-  
14 tronic means, including transmission and display, in-  
15 cluding via the Internet.

16 (3) **EXECUTIVE AGENCY.**—The term “Executive  
17 agency” has the meaning given the term in section  
18 105 of title 5, United States Code.

19 **SEC. 4. UNITED STATES INTERNATIONAL CYBERSPACE**  
20 **POLICY.**

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

G:\M16\MCCAUL\MCCAUL\_014.XML

8

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

4 (2) respects privacy and guards against decep-  
5 tion, fraud, and theft.

6 (b) IMPLEMENTATION.—In implementing the policy  
7 described in subsection (a), the President, in consultation  
8 with outside actors, including private sector companies,  
9 nongovernmental organizations, security researchers, and  
10 other relevant stakeholders, in the conduct of bilateral and  
11 multilateral relations, shall pursue the following objectives:

12 (1) Clarifying the applicability of international  
13 laws and norms to the use of ICT.

14 (2) Reducing and limiting the risk of escalation  
15 and retaliation in cyberspace, damage to critical in-  
16 frastructure, and other malicious cyber activity that  
17 impairs the use and operation of critical infrastruc-  
18 ture that provides services to the public.

19 (3) Cooperating with like-minded democratic  
20 countries that share common values and cyberspace  
21 policies with the United States, including respect for  
22 human rights, democracy, and the rule of law, to ad-  
23 vance such values and policies internationally.

24 (4) Encouraging the responsible development of  
25 new, innovative technologies and ICT products that

G:\M16\MCCAUL\MCCAUL\_014.XML

1 strengthen a secure Internet architecture that is ac-  
2 cessible to all.

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  
7 knowingly support, cyber-enabled theft of intel-  
8 lectual property, including trade secrets or  
9 other confidential business information, with  
10 the intent of providing competitive advantages  
11 to companies or commercial sectors.

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

16 (C) Countries should not conduct or know-  
17 ingly support ICT activity that, contrary to  
18 international law, intentionally damages or oth-  
19 erwise impairs the use and operation of critical  
20 infrastructure providing services to the public,  
21 and should take appropriate measures to pro-  
22 tect their critical infrastructure from ICT  
23 threats.

24 (D) Countries should not conduct or know-  
25 ingly support malicious international activity

G:\M16\MCCAUL\MCCAUL\_014.XML

10

1 that, contrary to international law, harms the  
2 information systems of authorized emergency  
3 response teams (also known as “computer  
4 emergency response teams” or “cybersecurity  
5 incident response teams”) of another country or  
6 authorize emergency response teams to engage  
7 in malicious international activity.

8 (E) Countries should respond to appro-  
9 priate requests for assistance to mitigate mali-  
10 cious ICT activity emanating from their terri-  
11 tory and aimed at the critical infrastructure of  
12 another country.

13 (F) Countries should not restrict cross-bor-  
14 der data flows or require local storage or proc-  
15 essing of data.

16 (G) Countries should protect the exercise  
17 of human rights and fundamental freedoms on  
18 the Internet and commit to the principle that  
19 the human rights that people have offline  
20 should also be protected online.

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



G:\M16\MCCAUL\MCCAUL\_014.XML

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

2 (a) IN GENERAL.—Section 1 of the State Depart-  
3 ment Basic Authorities Act of 1956 (22 U.S.C. 2651a)  
4 is amended—

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

7 (2) by inserting after subsection (f) the fol-  
8 lowing:

9 “(g) OFFICE OF INTERNATIONAL CYBERSPACE POL-  
10 ICY.—

11 “(1) IN GENERAL.—There is established, within  
12 the Department of State, an Office of International  
13 Cyberspace Policy (referred to in this subsection as  
14 the ‘Office’). The head of the Office shall have the  
15 rank and status of ambassador and shall be ap-  
16 pointed by the President, by and with the advice and  
17 consent of the Senate.

18 “(2) DUTIES.—

19 “(A) IN GENERAL.—The head of the Of-  
20 fice shall perform such duties and exercise such  
21 powers as the Secretary of State shall prescribe,  
22 including implementing the policy of the United  
23 States described in section 4 of the Cyber Di-  
24 plomacy Act of 2019.

G:\M\16\MCCAUL\MCCAUL\_014.XML

12

1           “(B) DUTIES DESCRIBED.—The principal  
2           duties and responsibilities of the head of the  
3           Office shall be—

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

9                   “(ii) to lead the Department of  
10                  State’s diplomatic cyberspace efforts, in-  
11                  cluding efforts relating to international cy-  
12                  bersecurity, Internet access, Internet free-  
13                  dom, digital economy, cybercrime, deter-  
14                  rence and international responses to cyber  
15                  threats, and other issues that the Sec-  
16                  retary assigns to the Office;

17                  “(iii) to promote an open, interoper-  
18                  able, reliable, unfettered, and secure infor-  
19                  mation and communications technology in-  
20                  frastructure globally;

21                  “(iv) to represent the Secretary of  
22                  State in interagency efforts to develop and  
23                  advance the policy described in section 4 of  
24                  the Cyber Diplomacy Act of 2019;

G:\M\16\MCCAUL\MCCAUL\_014.XML

1           “(v) to coordinate cyberspace efforts  
2           and other relevant functions, including  
3           countering terrorists’ use of cyberspace,  
4           within the Department of State and with  
5           other components of the United States  
6           Government;

7           “(vi) to act as a liaison to public and  
8           private sector entities on relevant inter-  
9           national cyberspace issues;

10          “(vii) to lead United States Govern-  
11          ment efforts to establish a global deter-  
12          rence framework for malicious cyber activ-  
13          ity;

14          “(viii) to develop and execute adver-  
15          sary-specific strategies to influence adver-  
16          sary decisionmaking through the imposi-  
17          tion of costs and deterrence strategies, in  
18          coordination with other relevant Executive  
19          agencies;

20          “(ix) to advise the Secretary and co-  
21          ordinate with foreign governments on ex-  
22          ternal responses to national-security-level  
23          cyber incidents, including coordination on  
24          diplomatic response efforts to support al-  
25          lies threatened by malicious cyber activity,

1 in conjunction with members of the North  
2 Atlantic Treaty Organization and other  
3 like-minded countries;

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

11 “(xi) to promote the building of for-  
12 eign capacity to protect the global network  
13 with the goal of enabling like-minded par-  
14 ticipation in deterrence frameworks;

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

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

24 “(xiv) to promote cross-border flow of  
25 data and combat international initiatives

G:\M16\MCCAUL\MCCAUL\_014.XML

15

1 seeking to impose unreasonable require-  
2 ments on United States businesses;

3 “(xv) to promote international policies  
4 to protect the integrity of United States  
5 and international telecommunications in-  
6 frastructure from foreign-based, cyber-en-  
7 abled threats;

8 “(xvi) to lead engagement, in coordi-  
9 nation with Executive agencies, with for-  
10 eign governments on relevant international  
11 cyberspace and digital economy issues as  
12 described in the Cyber Diplomacy Act of  
13 2019;

14 “(xvii) to promote international poli-  
15 cies to secure radio frequency spectrum for  
16 United States businesses and national se-  
17 curity needs;

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

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

G:\M16\MCCAUL\MCCAUL\_014.XML

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

5                   “(xxi) to consult, as appropriate, with  
6                   other Executive agencies with related func-  
7                   tions vested in such Executive agencies by  
8                   law.

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

12                  “(A) cybersecurity and other relevant  
13                  cyberspace issues; and

14                  “(B) international diplomacy.

15                  “(4) ORGANIZATIONAL PLACEMENT.—During  
16                  the 4-year period beginning on the date of the enact-  
17                  ment of the Cyber Diplomacy Act of 2019, the head  
18                  of the Office shall report to the Under Secretary for  
19                  Political Affairs or to an official holding a higher po-  
20                  sition than the Under Secretary for Political Affairs  
21                  in the Department of State. After the conclusion of  
22                  such period, the head of the Office shall report to  
23                  an appropriate Under Secretary or to an official  
24                  holding a higher position than Under Secretary.

G:\M16\MCCAUL\MCCAUL\_014.XML

17

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

3           “(A) the Office from being elevated to a  
4 Bureau within the Department of State; or

5           “(B) the head of the Office from being ele-  
6 vated to an Assistant Secretary, if such an As-  
7 sistant Secretary position does not increase the  
8 number of Assistant Secretary positions at the  
9 Department above the number authorized under  
10 subsection (c)(1).”.

11       (b) SENSE OF CONGRESS.—It is the sense of Con-  
12 gress that the Office of International Cyberspace Policy  
13 established under section 1(g) of the State Department  
14 Basic Authorities Act of 1956, as added by subsection (a),  
15 should be a Bureau of the Department of State and the  
16 head of such Office should report directly to the Secretary  
17 of State or Deputy Secretary of State.

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

1 **SEC. 6. INTERNATIONAL CYBERSPACE EXECUTIVE AR-**  
2 **RANGEMENTS.**

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

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

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

10 (2) in subsection (e)(2)(B), by adding at the  
11 end the following:

12 “(iii) A bilateral or multilateral cyberspace  
13 agreement.”;

14 (3) by redesignating subsection (f) as sub-  
15 section (g); and

16 (4) by inserting after subsection (e) the fol-  
17 lowing:

18 “(f) With respect to any bilateral or multilateral  
19 cyberspace agreement under subsection (e)(2)(B)(iii) and  
20 the information required to be transmitted to Congress  
21 under subsection (a), or with respect to any arrangement  
22 that seeks to secure commitments on responsible country  
23 behavior in cyberspace consistent with section 4(b)(5) of  
24 the Cyber Diplomacy Act of 2019, the Secretary of State  
25 shall provide an explanation of such arrangement, includ-  
26 ing—



G:\M16\MCCAUL\MCCAUL\_014.XML

1 “(1) the purpose of such arrangement;

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

4 “(3) how such arrangement will be imple-  
5 mented.”.

6 (c) STATUS REPORT.—During the 5-year period im-  
7 mediately following the transmittal to Congress of an  
8 agreement described in section 112b(e)(2)(B)(iii) of title  
9 1, United States Code, as added by subsection (b)(2), or  
10 until such agreement has been discontinued, if discon-  
11 tinued within 5 years, the President shall—

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

15 (2) describe the steps that the United States  
16 has taken or plans to take to ensure that all such  
17 commitments are fulfilled.

18 (d) EXISTING EXECUTIVE ARRANGEMENTS.—Not  
19 later than 180 days after the date of the enactment of  
20 this Act, the Secretary of State shall brief the appropriate  
21 congressional committees regarding any executive bilateral  
22 or multilateral cyberspace arrangement in effect before the  
23 date of enactment of this Act, including—

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

G:\M16\MCCAUL\MCCAUL\_014.XML

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

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

22 (12) any other similar bilateral or multilateral  
23 arrangement announced before such date of enact-  
24 ment.

G:\M16\MCCAUL\MCCAUL\_014.XML

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

2 (a) STRATEGY REQUIRED.—Not later than 1 year  
3 after the date of the enactment of this Act, the President,  
4 acting through the Secretary of State, and in coordination  
5 with the heads of other relevant Federal departments and  
6 agencies, shall develop a strategy relating to United States  
7 engagement with foreign governments on international  
8 norms with respect to responsible state behavior in cyber-  
9 space.

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

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

14 (2) A plan of action to guide the diplomacy of  
15 the Department of State with regard to foreign  
16 countries, including—

17 (A) conducting bilateral and multilateral  
18 activities to develop norms of responsible coun-  
19 try behavior in cyberspace consistent with the  
20 objectives under section 4(b)(5); and

21 (B) reviewing the status of existing efforts  
22 in relevant multilateral fora, as appropriate, to  
23 obtain commitments on international norms in  
24 cyberspace.

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

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

7                   (A) United States national security;

8                   (B) Federal and private sector cyberspace  
9 infrastructure of the United States;

10                  (C) intellectual property in the United  
11 States; and

12                  (D) the privacy of citizens of the United  
13 States.

14           (5) A review of policy tools available to the  
15 President to deter and de-escalate tensions with for-  
16 eign countries, state-sponsored actors, and private  
17 actors regarding threats in cyberspace, the degree to  
18 which such tools have been used, and whether such  
19 tools have been effective deterrents.

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

23           (7) A plan of action, developed in consultation  
24 with relevant Federal departments and agencies as  
25 the President may direct, to guide the diplomacy of

1 the Department of State with regard to inclusion of  
2 cyber issues in mutual defense agreements.

3 (c) FORM OF STRATEGY.—

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

8 (2) CLASSIFIED ANNEX.—The strategy required  
9 under subsection (a) may include a classified annex,  
10 consistent with United States national security inter-  
11 ests, if the Secretary of State determines that such  
12 annex is appropriate.

13 (d) BRIEFING.—Not later than 30 days after the  
14 completion of the strategy required under subsection (a),  
15 the Secretary of State shall brief the appropriate congres-  
16 sional committees on the strategy, including any material  
17 contained in a classified annex.

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

20 (1) not later than 90 days after any material  
21 change to United States policy described in such  
22 strategy; and

23 (2) not later than 1 year after the inauguration  
24 of each new President.

G:\M16\MCCAUL\MCCAUL\_014.XML

1 (f) PREEXISTING REQUIREMENT.—The Rec-  
2 ommendations to the President on Protecting American  
3 Cyber Interests through International Engagement, pre-  
4 pared by the Office of the Coordinator for Cyber Issues  
5 on May 31, 2018, pursuant to section 3(c) of Executive  
6 Order 13800 (82 Fed. Reg. 22391), shall be deemed to  
7 satisfy the requirement under subsection (a).

8 **SEC. 8. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS**  
9 **PRACTICES.**

10 Section 116 of the Foreign Assistance Act of 1961  
11 (22 U.S.C. 2151n) is amended by adding at the end the  
12 following:

13 “(h)(1) The report required under subsection (d)  
14 shall include an assessment of freedom of expression with  
15 respect to electronic information in each foreign country  
16 that includes the following:

17 “(A) An assessment of the extent to which gov-  
18 ernment authorities in the country inappropriately  
19 attempt to filter, censor, or otherwise block or re-  
20 move nonviolent expression of political or religious  
21 opinion or belief through the Internet, including  
22 electronic mail, and a description of the means by  
23 which such authorities attempt to inappropriately  
24 block or remove such expression.

1           “(B) An assessment of the extent to which gov-  
2 ernment authorities in the country have persecuted  
3 or otherwise punished, arbitrarily and without due  
4 process, an individual or group for the nonviolent ex-  
5 pression of political, religious, or ideological opinion  
6 or belief through the Internet, including electronic  
7 mail.

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

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

1       “(2) In compiling data and making assessments  
2 under paragraph (1), United States diplomatic personnel  
3 should consult with relevant entities, including human  
4 rights organizations, the private sector, the governments  
5 of like-minded countries, technology and Internet compa-  
6 nies, and other appropriate nongovernmental organiza-  
7 tions or entities.

8       “(3) In this subsection—

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

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

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

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

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

22       Not later than 1 year after the date of the enactment  
23 of this Act, the Comptroller General of the United States  
24 shall submit a report and provide a briefing to the appro-  
25 priate congressional committees that includes—



G:\M16\MCCAUL\MCCAUL\_014.XML

1 (1) an assessment of the extent to which United  
2 States diplomatic processes and other efforts with  
3 foreign countries, including through multilateral  
4 fora, bilateral engagements, and negotiated cyber-  
5 space agreements, advance the full range of United  
6 States interests in cyberspace, including the policy  
7 described in section 4;

8 (2) an assessment of the Department of State's  
9 organizational structure and approach to managing  
10 its diplomatic efforts to advance the full range of  
11 United States interests in cyberspace, including a re-  
12 view of—

13 (A) the establishment of a bureau in the  
14 Department of State to lead the Department's  
15 international cyber mission;

16 (B) the current or proposed diplomatic  
17 mission, structure, staffing, funding, and activi-  
18 ties of the bureau;

19 (C) how the establishment of the bureau  
20 has impacted or is likely to impact the structure  
21 and organization of the Department; and

22 (D) what challenges, if any, the Depart-  
23 ment has faced or will face in establishing such  
24 bureau; and

G:\M16\MCCAUL\MCCAUL\_014.XML

28

1           (3) any other matters determined relevant by  
2           the Comptroller General.

3 **SEC. 10. SENSE OF CONGRESS ON CYBERSECURITY SANC-**  
4 **TIONS AGAINST NORTH KOREA AND CYBER-**  
5 **SECURITY LEGISLATION IN VIETNAM.**

6           It is the sense of Congress that—

7           (1) the President should designate all entities  
8           that knowingly engage in significant activities under-  
9           mining cybersecurity through the use of computer  
10          networks or systems against foreign persons, govern-  
11          ments, or other entities on behalf of the Government  
12          of North Korea, consistent with section 209(b) of  
13          the North Korea Sanctions and Policy Enhancement  
14          Act of 2016 (22 U.S.C. 9229(b));

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

17                 (A) may not be consistent with inter-  
18                 national trade standards; and

19                 (B) may endanger the privacy of citizens  
20                 of Vietnam; and

21          (3) the Government of Vietnam should work  
22          with the United States and other countries to ensure  
23          that such law meets all relevant international stand-  
24          ards.

G:\M\16\MCCAUL\MCCAUL\_014.XML

1 **SEC. 11. RULE OF CONSTRUCTION.**

2 (a) **RULE OF CONSTRUCTION.**—Nothing in this Act  
3 may be construed to infringe upon the related functions  
4 of any Executive agency vested in such agency under any  
5 provision of law.





IV

116TH CONGRESS  
1ST SESSION

# H. RES. 156

Calling for accountability and justice for the assassination of Boris Nemtsov.

---

## IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 27, 2019

Mr. ENGEL (for himself, Mr. McCAUL, Mr. MALINOWSKI, and Ms. CHENEY)  
submitted the following resolution; which was referred to the Committee  
on Foreign Affairs

---

# RESOLUTION

Calling for accountability and justice for the assassination  
of Boris Nemtsov.

Whereas Boris Nemtsov was a Russian statesman who, over 25 years of public service, served as a Member of Parliament, Governor of the Nizhny Novgorod Region, and First Deputy Prime Minister of Russia;

Whereas throughout his life, Boris Nemtsov showed an unwavering commitment to the ideals of democracy, freedom, and the rule of law, and to upholding the rights and dignity of Russian citizens;

Whereas Boris Nemtsov was a powerful voice in opposition to the authoritarianism and corruption of Vladimir Putin's government, publicizing its abuses, leading street protests against election fraud and the war on Ukraine, and suc-

cessfully advocating for international sanctions on human rights violators;

Whereas Boris Nemtsov was co-chairman of a leading opposition party, won election to the Yaroslavl Regional Duma in 2013, and was planning to run for the Russian Parliament in 2016 and challenge Vladimir Putin for the Presidency in 2018;

Whereas, on the evening of February 27, 2015, Boris Nemtsov was shot in the back and killed as he walked across Bolshoi Moskvoretsky Bridge near the Kremlin in Moscow;

Whereas, on March 7 and 8, 2015, Russian authorities arrested five individuals, all of them natives of the Chechen Republic, on suspicion of carrying out the assassination, while a sixth suspect allegedly blew himself up during the attempted arrest;

Whereas the defendants were tried at the Moscow District Military Court, which on June 29, 2017, found them guilty of carrying out the assassination of Boris Nemtsov, and on July 13, 2017, sentenced them to different prison terms;

Whereas at the time of the assassination, the now-convicted gunman, Zaur Dadayev, was serving as a Lieutenant in the Internal Troops of the Interior Ministry of the Russian Federation and as Deputy Battalion Commander in the “Sever” (“North”) Regiment stationed in the Chechen Republic, under the command of the Internal Troops Commander, General Viktor Zolotov, and the Kremlin-backed head of the Chechen Republic, Ramzan Kadyrov;

Whereas Ramzan Kadyrov has called Lieutenant Zaur Dadayev a “true patriot” and has publicly referred to Boris Nemtsov as an “enemy of Russia”;

Whereas by Decree No. 115 issued on March 8, 2015, President Vladimir Putin awarded Ramzan Kadyrov the Order of Honor;

Whereas according to reports published in the RosBusinessConsulting (RBC) newspaper on January 20, 2016, General Alexander Bastrykin, chairman of the Investigative Committee of the Russian Federation, has on two occasions prevented investigators from indicting Major Ruslan Geremeyev, Battalion Commander in the “Sever” (“North”) Regiment of the Internal Troops of the Ministry of Internal Affairs of the Russian Federation stationed in the Chechen Republic and a close associate of Ramzan Kadyrov, as an organizer in the assassination;

Whereas according to reports published in Novaya Gazeta newspaper on December 9, 2016, operatives of the Federal Security Service of the Russian Federation in the Chechen Republic have failed to serve Major Ruslan Geremeyev with a summons for questioning as a witness, reporting to their superiors that on the sole occasion they attempted to do so, “nobody opened the door”;

Whereas despite requests from the legal team representing Boris Nemtsov’s family, the Investigative Committee of the Russian Federation and the Moscow District Military Court have refused to question high-ranking persons of interest, including Ramzan Kadyrov and General Viktor Zolotov;

Whereas the Investigative Committee of the Russian Federation has, to this day, not issued any indictments against

the organizers or masterminds of the assassination of Boris Nemtsov, with the exception of Major Ruslan Geremeyev's driver, Ruslan Mukhudinov, who is named alongside "other unidentified persons";

Whereas the Investigative Committee of the Russian Federation and the Moscow District Military Court have refused to classify the assassination of Boris Nemtsov under Article 277 of the Criminal Code as "encroachment on the life of a statesman or a public figure," choosing instead Article 105 that deals with common domestic murders;

Whereas throughout the proceedings at the Moscow District Military Court, the judge repeatedly disallowed questions relating to political motives behind the assassination;

Whereas the Federal Protective Service of the Russian Federation has refused to release video footage from the security cameras on Bolshoi Moskvoretsky Bridge from the night of the assassination, claiming in a letter to State Duma Member Dmitry Gudkov on November 6, 2015, that the bridge next to the Kremlin is "not a protected object";

Whereas, on May 18, 2017, the Parliamentary Assembly of the Council of Europe appointed Lithuanian Member of Parliament Emanuelis Zingeris as its special rapporteur on the need to shed light on the background of the murder of Boris Nemtsov, with a mandate to review and report on the case and on the progress of the official Russian investigation;

Whereas, on May 24, 2018, the Russian Foreign Ministry informed Emanuelis Zingeris that he is forbidden from entering the Russian Federation;

Whereas, at its 27th annual session held on July 7 through 11, 2018, the Parliamentary Assembly of the Organization for Security and Cooperation in Europe (OSCE) adopted a resolution urging Russian authorities to “undertake a new, full and thorough investigation into the February 2015 assassination of Boris Nemtsov”;

Whereas, on July 8, 2018, the Parliamentary Assembly of the Organization for Security and Cooperation in Europe held a public event to discuss the need for OSCE oversight of the official Russian investigation into the assassination of Boris Nemtsov;

Whereas the United States and the Russian Federation are full members of the Organization for Security and Cooperation in Europe;

Whereas the OSCE Moscow Document has established that “issues relating to human rights, fundamental freedoms, democracy and the rule of law . . . are matters of direct and legitimate concern to all participating States and do not belong exclusively to the internal affairs of the State concerned”;

Whereas, on February 27, 2018, Washington, DC, designated the street in front of the Embassy of the Russian Federation as “Boris Nemtsov Plaza” to honor Mr. Nemtsov; and

Whereas, on February 22, 2019, the President of the Parliamentary Assembly of the OSCE, George Tsereteli, appointed Swedish Member of Parliament and Vice President of the Assembly Margareta Cederfelt as the rapporteur on the investigation of the assassination of Boris Nemtsov, with a mandate to review and report on



the case and on the progress of the official Russian investigation: Now, therefore, be it

1       *Resolved*, That the House of Representatives—

2               (1) condemns Vladimir Putin and his regime  
3       for targeting political opponents and covering up the  
4       assassination of Boris Nemtsov, a Russian opposi-  
5       tion leader who worked to advance democracy and  
6       human rights in Russia;

7               (2) urges the United States Government, in all  
8       its interactions with the Government of the Russian  
9       Federation, to raise the case of the assassination of  
10       Boris Nemtsov and underscore the necessity of  
11       bringing the organizers and masterminds to justice;

12              (3) supports the efforts by the Organization for  
13       Security and Cooperation in Europe (OSCE) and its  
14       Parliamentary Assembly to initiate oversight of the  
15       official Russian investigation into the assassination  
16       of Boris Nemtsov;

17              (4) calls on the Government of the Russian  
18       Federation to allow an impartial international inves-  
19       tigation of the assassination of Boris Nemtsov and  
20       to cooperate with the Parliamentary Assembly of the  
21       OSCE and the Parliamentary Assembly of the Coun-  
22       cil of Europe in their ongoing inquiries over this  
23       case;

1           (5) calls on the Secretary of State and the Sec-  
2           retary of the Treasury to use their authority under  
3           the Sergei Magnitsky Rule of Law Accountability  
4           Act of 2012 (title IV of Public Law 112–208) and  
5           the Global Magnitsky Human Rights Accountability  
6           Act (subtitle F of title XII of Public Law 114–328)  
7           to designate individuals whom they determine to  
8           have been involved in the assassination of Boris  
9           Nemtsov as perpetrators, organizers, or master-  
10          minds, on the list of specially designated nationals  
11          and blocked persons maintained by the Office of  
12          Foreign Assets Control of the Department of the  
13          Treasury, freezing their assets and making them in-  
14          eligible to receive United States visas; and

15          (6) calls on the Secretary of State, in consulta-  
16          tion with the Director of National Intelligence, to  
17          prepare and submit to Congress a report detailing  
18          the circumstances of the February 27, 2015, assas-  
19          sination of Boris Nemtsov, including the list of indi-  
20          viduals whom they determine to have been involved  
21          in the assassination as perpetrators, organizers, or  
22          masterminds, and identifying what measures, if any,  
23          have been taken by the Government of the Russian  
24          Federation to investigate this crime and bring its

- 1 perpetrators, organizers, and masterminds to justice,
- 2 and evaluating the effectiveness of such measures.

○

G:\CMTE\FAM\HR156\_A1.XML

**AMENDMENT TO H. RES. 156**  
**OFFERED BY MR. MALINOWSKI OF NEW JERSEY**

In the 11th clause of the preamble, insert “and Russian State Duma Member Adam Delimkhanov” after “Ramzan Kadyrov”.

In the 13th clause of the preamble, strike “and General Victor Zolotov” and insert “, General Victor Zolotov, and Adam Delimkhanov”.



G:\M\16\MALIN\MALINJ\_011.XML

**AMENDMENT TO H. RES. 156**  
**OFFERED BY MR. MALINOWSKI OF NEW JERSEY**

Page 7, line 14, strike “; and” and insert “;”.

Page 8, line 2, strike the period at the end and insert “; and”.

Page 8, after line 2, insert the following:

- 1           (7) urges the Secretary of State to take all possible steps to—
- 2
- 3           (A) investigate the business activities of
- 4           Ramzan Kadyrov and any entities controlled by
- 5           Ramzan Kadyrov outside the Russian Federation; and
- 6
- 7           (B) determine whether any such activities,
- 8           or any entities facilitating such activities, are in
- 9           violation of the sanctions imposed on Ramzan
- 10          Kadyrov pursuant to the authorities provided
- 11          by the Global Magnitsky Human Rights Accountability Act (22 U.S.C. 2656 note).
- 12





116TH CONGRESS  
1ST SESSION

# H. R. 596

To prohibit United States Government recognition of Russia’s annexation of Crimea.

---

IN THE HOUSE OF REPRESENTATIVES

JANUARY 16, 2019

Mr. CONNOLLY (for himself and Mr. CHABOT) introduced the following bill; which was referred to the Committee on Foreign Affairs

---

## A BILL

To prohibit United States Government recognition of Russia’s annexation of Crimea.

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 “Crimea Annexation  
5 Non-recognition Act”.

6 **SEC. 2. PROHIBITION AGAINST UNITED STATES RECOGNI-**  
7 **TION OF RUSSIA’S ANNEXATION OF CRIMEA.**

8 (a) STATEMENT OF POLICY.—It is the policy of the  
9 United States not to recognize the de jure or de facto sov-

1 ereignty of the Russian Federation over Crimea, its air-  
2 space, or its territorial waters.

3 (b) PROHIBITION.—In accordance with subsection  
4 (a), no Federal department or agency may take any action  
5 or extend any assistance that recognizes or implies rec-  
6 ognition of the de jure or de facto sovereignty of the Rus-  
7 sian Federation over Crimea, its airspace, or its territorial  
8 waters.

9 (c) WAIVER.—The President may waive subsection  
10 (a) or (b) if the President determines that it is vital to  
11 the national security interests of the United States to do  
12 so.

○

**AMENDMENT IN THE NATURE OF A SUBSTITUTE  
TO H.R. 596  
OFFERED BY MR. CONNOLLY OF VIRGINIA**

Strike all after the enacting clause and insert the following:

**1 SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Crimea Annexation  
3 Non-recognition Act”.

**4 SEC. 2. PROHIBITION AGAINST UNITED STATES RECOGNITION OF THE RUSSIAN FEDERATION'S CLAIM OF SOVEREIGNTY OVER CRIMEA.**

7 (a) STATEMENT OF POLICY.—It is the policy of the  
8 United States not to recognize the Russian Federation’s  
9 claim of sovereignty over Crimea, its airspace, or its territorial waters.  
10

11 (b) PROHIBITION.—In accordance with subsection  
12 (a), no Federal department or agency may take any action  
13 or extend any assistance that implies recognition of the  
14 Russian Federation’s claim of sovereignty over Crimea, its  
15 airspace, or its territorial waters.

16 (c) WAIVER.—The President may waive the prohibition in subsection (b) on a case-by-case basis if the Presi-



G:\M16\CONNOL\CONNOL\_022.XML

2

1 dent determines that it is vital to the national security  
2 interests of the United States to do so.

Amend the title so as to read: "A bill to prohibit  
United States Government recognition of the Russian  
Federation's claim of sovereignty over Crimea, and for  
other purposes."





116TH CONGRESS  
1ST SESSION

# H. R. 295

To increase the role of the financial industry in combating human trafficking.

---

## IN THE HOUSE OF REPRESENTATIVES

JANUARY 8, 2019

Mr. FITZPATRICK (for himself, Mr. KEATING, Mr. MCCAUL, and Mrs. CAROLYN B. MALONEY of New York) introduced the following bill; which was referred to the Committee on Foreign Affairs, and in addition to the Committee on Financial Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

## A BILL

To increase the role of the financial industry in combating human trafficking.

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 “End Banking for  
5 Human Traffickers Act of 2019”.

6 **SEC. 2. INCREASING THE ROLE OF THE FINANCIAL INDUS-**  
7 **TRY IN COMBATING HUMAN TRAFFICKING.**

8 (a) TREASURY AS A MEMBER OF THE PRESIDENT’S  
9 INTERAGENCY TASK FORCE TO MONITOR AND COMBAT

1 TRAFFICKING.—Section 105(b) of the Victims of Traf-  
2 ficking and Violence Protection Act of 2000 (22 U.S.C.  
3 7103(b)) is amended by inserting “the Secretary of the  
4 Treasury,” after “the Secretary of Education,”.

5 (b) REQUIRED REVIEW OF PROCEDURES.—Not later  
6 than 180 days after the date of the enactment of this Act,  
7 the Financial Institutions Examination Council, in con-  
8 sultation with the Secretary of the Treasury, the private  
9 sector, victims of severe forms of trafficking in persons,  
10 advocates of persons at risk of becoming victims of severe  
11 forms of trafficking in persons, and appropriate law en-  
12 forcement agencies, shall—

13 (1) review and enhance training and examina-  
14 tions procedures to improve the capabilities of anti-  
15 money laundering and countering the financing of  
16 terrorism programs to detect financial transactions  
17 relating to severe forms of trafficking in persons;

18 (2) review and enhance procedures for referring  
19 potential cases relating to severe forms of trafficking  
20 in persons to the appropriate law enforcement agen-  
21 cy; and

22 (3) determine, as appropriate, whether require-  
23 ments for financial institutions are sufficient to de-  
24 tect and deter money laundering relating to severe  
25 forms of trafficking in persons.

1 (c) INTERAGENCY TASK FORCE RECOMMENDATIONS  
2 TARGETING MONEY LAUNDERING RELATED TO HUMAN  
3 TRAFFICKING.—

4 (1) IN GENERAL.—Not later than 270 days  
5 after the date of the enactment of this Act, the  
6 Interagency Task Force To Monitor and Combat  
7 Trafficking shall submit to the Committee on Finan-  
8 cial Services and the Committee on the Judiciary of  
9 the House of Representatives, the Committee on  
10 Banking, Housing, and Urban Affairs and the Com-  
11 mittee on the Judiciary of the Senate, and the head  
12 of each appropriate Federal banking agency—

13 (A) an analysis of anti-money laundering  
14 efforts of the United States Government and  
15 United States financial institutions relating to  
16 severe forms of trafficking in persons; and

17 (B) appropriate legislative, administrative,  
18 and other recommendations to strengthen ef-  
19 forts against money laundering relating to se-  
20 vere forms of trafficking in persons.

21 (2) REQUIRED RECOMMENDATIONS.—The rec-  
22 ommendations under paragraph (1) shall include—

23 (A) feedback from financial institutions on  
24 best practices of successful programs to combat  
25 severe forms of trafficking in persons currently

1 in place that may be suitable for broader adop-  
2 tion by similarly situated financial institutions;

3 (B) feedback from stakeholders, including  
4 victims of severe forms of trafficking in per-  
5 sons, advocates of persons at risk of becoming  
6 victims of severe forms of trafficking in per-  
7 sons, and financial institutions, on policy pro-  
8 posals derived from the analysis conducted by  
9 the task force referred to in paragraph (1) that  
10 would enhance the efforts and programs of fi-  
11 nancial institutions to detect and deter money  
12 laundering relating to severe forms of traf-  
13 ficking in persons, including any recommended  
14 changes to internal policies, procedures, and  
15 controls relating to severe forms of trafficking  
16 in persons;

17 (C) any recommended changes to training  
18 programs at financial institutions to better  
19 equip employees to deter and detect money  
20 laundering relating to severe forms of traf-  
21 ficking in persons;

22 (D) any recommended changes to expand  
23 information sharing relating to severe forms of  
24 trafficking in persons among financial institu-  
25 tions and between such financial institutions,

1 appropriate law enforcement agencies, and ap-  
2 propriate Federal agencies; and

3 (E) recommended changes, if necessary, to  
4 existing statutory law to more effectively detect  
5 and deter money laundering relating to severe  
6 forms of trafficking in persons, where such  
7 money laundering involves the use of emerging  
8 technologies and virtual currencies.

9 (d) LIMITATION.—Nothing in this Act shall be con-  
10 strued to—

11 (1) grant rulemaking authority to the Inter-  
12 agency Task Force To Monitor and Combat Traf-  
13 ficking; or

14 (2) encourage financial institutions to deny  
15 services to victims of trafficking, victims of severe  
16 forms of trafficking in persons, or individuals not re-  
17 sponsible for promoting severe forms of trafficking  
18 in persons.

19 (e) DEFINITIONS.—As used in this section—

20 (1) the term “appropriate Federal banking  
21 agency” has the meaning given the term in section  
22 3(q) of the Federal Deposit Insurance Act (12  
23 U.S.C. 1813(q));

24 (2) the term “severe forms of trafficking in per-  
25 sons” has the meaning given such term in section

1 103 of the Trafficking Victims Protection Act of  
2 2000 (22 U.S.C. 7102);

3 (3) the term “Interagency Task Force To Mon-  
4 itor and Combat Trafficking” means the Interagency  
5 Task Force To Monitor and Combat Trafficking es-  
6 tablished by the President pursuant to section 105  
7 of the Victims of Trafficking and Violence Protec-  
8 tion Act of 2000 (22 U.S.C. 7103); and

9 (4) the term “law enforcement agency” means  
10 an agency of the United States, a State, or a polit-  
11 ical subdivision of a State, authorized by law or by  
12 a government agency to engage in or supervise the  
13 prevention, detection, investigation, or prosecution of  
14 any violation of criminal or civil law.

15 **SEC. 3. COORDINATION OF HUMAN TRAFFICKING ISSUES**  
16 **BY THE OFFICE OF TERRORISM AND FINAN-**  
17 **CIAL INTELLIGENCE.**

18 (a) FUNCTIONS.—Section 312(a)(4) of title 31,  
19 United States Code, is amended—

20 (1) by redesignating subparagraphs (E), (F),  
21 and (G) as subparagraphs (F), (G), and (H), respec-  
22 tively; and

23 (2) by inserting after subparagraph (D) the fol-  
24 lowing:

1           “(E) combating illicit financing relating to  
2           severe forms of trafficking in persons;”.

3           (b) INTERAGENCY COORDINATION.—Section 312(a)  
4 of title 31, United States Code, is amended by adding at  
5 the end the following:

6           “(8) INTERAGENCY COORDINATION.—The Sec-  
7           retary of the Treasury, after consultation with the  
8           Undersecretary for Terrorism and Financial Crimes,  
9           shall designate an office within the OTFI that shall  
10          coordinate efforts to combat the illicit financing of  
11          severe forms of trafficking in persons with—

12           “(A) other offices of the Department of the  
13          Treasury;

14           “(B) other Federal agencies, including—

15           “(i) the Office To Monitor and Com-  
16          bat Trafficking in Persons of the Depart-  
17          ment of State; and

18           “(ii) the Interagency Task Force To  
19          Monitor and Combat Trafficking;

20           “(C) State and local law enforcement agen-  
21          cies; and

22           “(D) foreign governments.”.

23           (c) DEFINITION.—Section 312(a) of title 31, United  
24 States Code, as amended by this section, is further amend-  
25 ed by adding at the end the following:



1           “(9) DEFINITION.—In this subsection, the term  
2           ‘severe forms of trafficking in persons’ has the  
3           meaning given such term in section 103 of the Traf-  
4           ficking Victims Protection Act of 2000 (22 U.S.C.  
5           7102).”.

6 **SEC. 4. ADDITIONAL REPORTING REQUIREMENT UNDER**  
7           **THE TRAFFICKING VICTIMS PROTECTION**  
8           **ACT OF 2000.**

9           Section 105(d)(7) of the Trafficking Victims Protec-  
10          tion Act of 2000 (22 U.S.C. 7103(d)(7)) is amended—

11           (1) in the matter preceding subparagraph (A)—

12                   (A) by inserting “the Committee on Finan-  
13                   cial Services,” after “the Committee on Foreign  
14                   Affairs,”; and

15                   (B) by inserting “the Committee on Bank-  
16                   ing, Housing, and Urban Affairs,” after “the  
17                   Committee on Foreign Relations,”;

18           (2) in subparagraph (Q)(vii), by striking “;  
19           and” and inserting a semicolon;

20           (3) in subparagraph (R), by striking the period  
21           at the end and inserting “; and”; and

22           (4) by adding at the end the following:

23                   “(S) the efforts of the United States to  
24                   eliminate money laundering relating to severe  
25                   forms of trafficking in persons and the number

1 of investigations, arrests, indictments, and con-  
2 victions in money laundering cases with a nexus  
3 to severe forms of trafficking in persons.”.

4 **SEC. 5. MINIMUM STANDARDS FOR THE ELIMINATION OF**  
5 **TRAFFICKING.**

6 Section 108(b) of the Trafficking Victims Protection  
7 Act of 2000 (22 U.S.C. 7106(b)) is amended by adding  
8 at the end the following new paragraph:

9 “(13) Whether the government of the country,  
10 consistent with the capacity of the country, has in  
11 effect a framework to prevent financial transactions  
12 involving the proceeds of severe forms of trafficking  
13 in persons, and is taking steps to implement such a  
14 framework, including by investigating, prosecuting,  
15 convicting, and sentencing individuals who attempt  
16 or conduct such transactions.”.

○

**AMENDMENT IN THE NATURE OF A SUBSTITUTE  
TO H.R. 295  
OFFERED BY MR. ENGEL OF NEW YORK**

Strike all after the enacting clause and insert the following:

**1 SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “End Banking for  
3 Human Traffickers Act of 2019”.

**4 SEC. 2. INCREASING THE ROLE OF THE FINANCIAL INDUS-  
5 TRY IN COMBATING HUMAN TRAFFICKING.**

6 (a) REQUIRED REVIEW OF PROCEDURES.—Not later  
7 than 180 days after the date of the enactment of this Act,  
8 the Financial Institutions Examination Council, in con-  
9 sultation with the Secretary of the Treasury, the private  
10 sector, victims of severe forms of trafficking in persons,  
11 advocates of persons at risk of becoming victims of severe  
12 forms of trafficking in persons, and appropriate law en-  
13 forcement agencies, shall—

14 (1) review and enhance training and examina-  
15 tions procedures to improve the capabilities of anti-  
16 money laundering and countering the financing of  
17 terrorism programs to detect financial transactions  
18 relating to severe forms of trafficking in persons;

G:\M\16ENGE\ENGE\_027.XML

2

1           (2) review and enhance procedures for referring  
2           potential cases relating to severe forms of trafficking  
3           in persons to the appropriate law enforcement agen-  
4           cy; and

5           (3) determine, as appropriate, whether require-  
6           ments for financial institutions are sufficient to de-  
7           tect and deter money laundering relating to severe  
8           forms of trafficking in persons.

9           (b) INTERAGENCY TASK FORCE RECOMMENDATIONS  
10          TARGETING MONEY LAUNDERING RELATED TO HUMAN  
11          TRAFFICKING.—

12           (1) IN GENERAL.—Not later than 270 days  
13           after the date of the enactment of this Act, the  
14           Interagency Task Force To Monitor and Combat  
15           Trafficking shall submit to the Committee on Finan-  
16           cial Services and the Committee on the Judiciary of  
17           the House of Representatives, the Committee on  
18           Banking, Housing, and Urban Affairs and the Com-  
19           mittee on the Judiciary of the Senate, and the head  
20           of each appropriate Federal banking agency—

21           (A) an analysis of anti-money laundering  
22           efforts of the United States Government and  
23           United States financial institutions relating to  
24           severe forms of trafficking in persons; and

G:\M16\ENGEL\ENGEL\_027.XML

3

1 (B) appropriate legislative, administrative,  
2 and other recommendations to strengthen ef-  
3 forts against money laundering relating to se-  
4 vere forms of trafficking in persons.

5 (2) REQUIRED RECOMMENDATIONS.—The rec-  
6 ommendations under paragraph (1) shall include—

7 (A) feedback from financial institutions on  
8 best practices of successful programs to combat  
9 severe forms of trafficking in persons currently  
10 in place that may be suitable for broader adop-  
11 tion by similarly situated financial institutions;

12 (B) feedback from stakeholders, including  
13 victims of severe forms of trafficking in per-  
14 sons, advocates of persons at risk of becoming  
15 victims of severe forms of trafficking in per-  
16 sons, and financial institutions, on policy pro-  
17 posals derived from the analysis conducted by  
18 the task force referred to in paragraph (1) that  
19 would enhance the efforts and programs of fi-  
20 nancial institutions to detect and deter money  
21 laundering relating to severe forms of traf-  
22 ficking in persons, including any recommended  
23 changes to internal policies, procedures, and  
24 controls relating to severe forms of trafficking  
25 in persons;

G:\M\16\ENGEL\ENGEL\_027.XML

4

1 (C) any recommended changes to training  
2 programs at financial institutions to better  
3 equip employees to deter and detect money  
4 laundering relating to severe forms of traf-  
5 ficking in persons;

6 (D) any recommended changes to expand  
7 information sharing relating to severe forms of  
8 trafficking in persons among financial institu-  
9 tions and between such financial institutions,  
10 appropriate law enforcement agencies, and ap-  
11 propriate Federal agencies; and

12 (E) recommended changes, if necessary, to  
13 existing statutory law to more effectively detect  
14 and deter money laundering relating to severe  
15 forms of trafficking in persons, where such  
16 money laundering involves the use of emerging  
17 technologies and virtual currencies.

18 (e) LIMITATION.—Nothing in this Act shall be con-  
19 strued to—

20 (1) grant rulemaking authority to the Inter-  
21 agency Task Force To Monitor and Combat Traf-  
22 ficking; or

23 (2) encourage financial institutions to deny  
24 services to victims of trafficking, victims of severe  
25 forms of trafficking in persons, or individuals not re-

G:\M16\ENGEL\ENGEL\_027.XML

1       sponsible for promoting severe forms of trafficking  
2       in persons.

3       (d) DEFINITIONS.—As used in this section—

4           (1) the term “appropriate Federal banking  
5       agency” has the meaning given the term in section  
6       3(q) of the Federal Deposit Insurance Act (12  
7       U.S.C. 1813(q));

8           (2) the term “severe forms of trafficking in per-  
9       sons” has the meaning given such term in section  
10       103 of the Trafficking Victims Protection Act of  
11       2000 (22 U.S.C. 7102);

12          (3) the term “Interagency Task Force To Mon-  
13       itor and Combat Trafficking” means the Interagency  
14       Task Force To Monitor and Combat Trafficking es-  
15       tablished by the President pursuant to section 105  
16       of the Victims of Trafficking and Violence Protec-  
17       tion Act of 2000 (22 U.S.C. 7103); and

18          (4) the term “law enforcement agency” means  
19       an agency of the United States, a State, or a polit-  
20       ical subdivision of a State, authorized by law or by  
21       a government agency to engage in or supervise the  
22       prevention, detection, investigation, or prosecution of  
23       any violation of criminal or civil law.

G:\M16\ENGEL\ENGEL\_027.XML

6

1 **SEC. 3. COORDINATION OF HUMAN TRAFFICKING ISSUES**  
2 **BY THE OFFICE OF TERRORISM AND FINAN-**  
3 **CIAL INTELLIGENCE.**

4 (a) FUNCTIONS.—Section 312(a)(4) of title 31,  
5 United States Code, is amended—

6 (1) by redesignating subparagraphs (E), (F),  
7 and (G) as subparagraphs (F), (G), and (H), respec-  
8 tively; and

9 (2) by inserting after subparagraph (D) the fol-  
10 lowing:

11 “(E) combating illicit financing relating to  
12 severe forms of trafficking in persons;”.

13 (b) INTERAGENCY COORDINATION.—Section 312(a)  
14 of title 31, United States Code, is amended by adding at  
15 the end the following:

16 “(8) INTERAGENCY COORDINATION.—The Sec-  
17 retary of the Treasury, after consultation with the  
18 Undersecretary for Terrorism and Financial Crimes,  
19 shall designate an office within the OTFI that shall  
20 coordinate efforts to combat the illicit financing of  
21 severe forms of trafficking in persons with—

22 “(A) other offices of the Department of the  
23 Treasury;

24 “(B) other Federal agencies, including—



G:\M16\ENGEL\ENGEL\_027.XML

7

1                   “(i) the Office To Monitor and Com-  
2                   bat Trafficking in Persons of the Depart-  
3                   ment of State; and

4                   “(ii) the Interagency Task Force To  
5                   Monitor and Combat Trafficking;

6                   “(C) State and local law enforcement agen-  
7                   cies; and

8                   “(D) foreign governments.”.

9           (e) DEFINITION.—Section 312(a) of title 31, United  
10 States Code, as amended by this section, is further amend-  
11 ed by adding at the end the following:

12                   “(9) DEFINITION.—In this subsection, the term  
13                   ‘severe forms of trafficking in persons’ has the  
14                   meaning given such term in section 103 of the Traf-  
15                   ficking Victims Protection Act of 2000 (22 U.S.C.  
16                   7102).”.

17 **SEC. 4. ADDITIONAL REPORTING REQUIREMENT UNDER**  
18 **THE TRAFFICKING VICTIMS PROTECTION**  
19 **ACT OF 2000.**

20           Section 105(d)(7) of the Trafficking Victims Protec-  
21 tion Act of 2000 (22 U.S.C. 7103(d)(7)) is amended—

22                   (1) in the matter preceding subparagraph (A)—

23                   (A) by inserting “the Committee on Finan-  
24                   cial Services,” after “the Committee on Foreign  
25                   Affairs,”; and

G:\M\16\ENGEL\ENGEL\_027.XML

8

1 (B) by inserting “the Committee on Bank-  
 2 ing, Housing, and Urban Affairs,” after “the  
 3 Committee on Foreign Relations,”;

4 (2) in subparagraph (Q)—

5 (A) in clause (vii), by inserting “and” after  
 6 the semicolon; and

7 (B) in clause (viii), by striking “and” after  
 8 the semicolon;

9 (3) in subparagraph (R), by striking “and”  
 10 after the semicolon;

11 (4) in subparagraph (S), by striking the period  
 12 and inserting “; and”; and

13 (5) by adding at the end the following:

14 “(T) the efforts of the United States to  
 15 eliminate money laundering relating to severe  
 16 forms of trafficking in persons and the number  
 17 of investigations, arrests, indictments, and con-  
 18 victions in money laundering cases with a nexus  
 19 to severe forms of trafficking in persons.”.

20 **SEC. 5. MINIMUM STANDARDS FOR THE ELIMINATION OF**  
 21 **TRAFFICKING.**

22 Section 108(b) of the Trafficking Victims Protection  
 23 Act of 2000 (22 U.S.C. 7106(b)) is amended by adding  
 24 at the end the following new paragraph:

G:\M\16\ENGEL\ENGEL\_027.XML

9

1           “(13) Whether the government of the country,  
2           consistent with the capacity of the country, has in  
3           effect a framework to prevent financial transactions  
4           involving the proceeds of severe forms of trafficking  
5           in persons, and is taking steps to implement such a  
6           framework, including by investigating, prosecuting,  
7           convicting, and sentencing individuals who attempt  
8           or conduct such transactions.”.

Chairman ENGEL. At this time I recognize myself to speak on today's business.

We have five good measures before us today and I am pleased to support them all. The first measure I want to discuss is H. Res. 156, a resolution I authored with Ranking Member McCaul that calls for justice for the assassination of Boris Nemtsov.

Nemtsov was a brave advocate for democracy and free elections in Russia. Sadly, that put him right in Vladimir Putin's cross hairs.

Now he joins a long list of brave journalists, human rights activists, and political opponents murdered by Putin's henchmen in their quest to silence all criticism of the Kremlin and stamp out any perceived threat to Putin's authoritarian regime.

This resolution condemns the Kremlin's systematic targeting of its political opponents and it calls on the administration to implement Magnitsky Act sanctions on those responsible for Nemtsov's murder and cover up.

It also requires the administration to deliver to Congress a thorough report on Nemtsov's assassination. That is a critical part of this legislation because, sadly, the administration has not done nearly enough to give us much reason to stand up to Russia and call out Putin's thuggery.

So it is up to Congress to assert American leadership on this issue and Putin's strong arm tactics extend beyond the authoritarian rule in his own country. We have seen this all too clearly in Russia's malign actions with its neighbors, which brings me to our next measure.

But before I do that, I want to just personally tell you I have on my desk in my office a picture of me shaking hands with Boris Nemtsov. It is shocking. When we moved offices I saw that picture. I had forgotten about it.

He came and visited me and told me he was the opponent of Putin and that he was for free, independent elections and for a free Russia.

I was very, very impressed with him and thought, wow, this man is really special. Unfortunately, Putin thought so too and had him killed right in Moscow. But I remember him telling me about how he felt how important his work was, and I told him that I thought he was really working, not for just the people in Russia, but for people all over the world.

So I want to just mention that because it was quite an honor for me to meet Boris Nemtsov and, of course, just a few months later he was murdered.

And so it is just startling.

The Crimea Annexation Nonrecognition Act puts that conviction into law by stating that the United States will not recognize Russia's claims of sovereignty in Ukraine.

Putin's disrespect for independent, sovereign democracies is something we in the United States know all too well. By advancing this legislation we send a clear message to our Ukrainian partners and their neighbors. We stand with you. I support this bill and I urge my colleagues to do the same.

And just as an aside, I have been a strong supporter of Ukraine being admitted to NATO and I think we should pursue that down the road.

It is critical that we support our partners and allies whenever they are under threat and that brings me to our next measure, H. Res. 75. I want to thank Mr. McCaul, Ms. Bass, and Mr. Smith for joining me in this resolution that strongly condemns the January 2019 attack by the terrorist group Al-Shabaab in Nairobi, Kenya.

This horrific attack killed dozens of people, including American citizen Jason Spindler. Just last week, we saw another Al-Shabaab attack in Mogadishu, Somalia, claim the lives of nearly 30 people.

So this resolution rightly affirms that the United States supports our regional partners in their ongoing efforts to counter terrorism and violent extremism in the Horn of Africa. I hope all members will join me in supporting this measure.

Next, I would like to discuss the End Banking for Human Traffickers Act introduced by Mr. Fitzpatrick and Mr. Keating. It is horrible that in 2019, we still live in a world where human beings are held in slavery. It is a moral outrage.

So we need to be consistently evaluating our government's efforts on this issue and looking for areas where we can improve. This bill does just that by having the financial industry play a bigger role in tracking down human traffickers.

By connecting the industry with experts on human trafficking, banks and other financial institutions will be better equipped to spot suspect financial transactions that may be related to this heinous criminal enterprise.

This bill continues our fight against the scourge of human trafficking, and I urge my colleagues to join me in supporting it.

And finally, we turn to Ranking Member McCall's bill, the Cyber Diplomacy Act. Last Congress, I worked with Chairman Royce on this bill and we got it through this committee, the House, and the Senate Foreign Relations Committee with broad bipartisan support.

This Congress, Ranking Member McCaul has taken up that mantle and I am pleased to join him as we work to get this bill over the finish line and on the president's desk.

Cyberspace is an increasingly critical part of foreign policy and we desperately need to update our government agencies to reflect that reality.

America has significant interest in cybersecurity, the digital economy, issues of internet freedom, and we need to be engaging with the international community to articulate and protect those interests.

If we do not focus on all of these areas, we run the real risk of seeing authoritarian regimes like Russia and China playing a bigger role in determining the way the international community handles these issues.

So this bill would create a high-level Ambassador position at the State Department dedicated to this endeavor and require a comprehensive cyberspace strategy.

I am frustrated by the lack of progress on this issue at the State Department, and I hope they will work with us to ensure that this bill becomes law.

I hope my colleagues will join me in supporting this measure.

Thank you to all of our members for your hard work on these good bills before us today. As I said before, I am pleased to support them all.

And now, I recognize the ranking member, Mike McCaul of Texas, for his opening remarks.

Mr. MCCAUL. Thank you, Mr. Chairman.

Today, our committee will markup three important bills and two resolutions, the Cyber Diplomacy Act, which I introduced with you, Mr. Chairman. I want to thank you for working with me on that. It takes several steps to support an open and secure cyberspace. As chairman of Homeland Security, I elevated the mission at the Department of Homeland Security and I intend to do the same with you, sir, at the Department of State.

It establishes an ambassador at large to lead the State's cyber diplomacy efforts, outlines an international cyber policy to advance democratic principles and reject Russian and Chinese attempts to control and censor the internet.

It requires the State Department to provide assessments related to internet freedom, freedoms in other countries, and, as you know, Mr. Chairman, malicious cyber activity by State and non-State actors threatens our national security and harms our economic interests.

We understand the State Department has plans for a new cyber bureau, which varies a little bit from what our bill calls for. I pledge to work with the State Department and you, Mr. Chairman, and the Senate to find the best path forward to advance our shared goals of bolstering and elevating State's critical cyber mission.

I also want to thank Mr. Fitzpatrick and Mr. Keating for their bipartisan bill, the End Banking for Human Traffickers Act, which will help address the scourge of human trafficking.

This bill will help choke off traffickers' access to financial systems. It is time we put an end to this modern-day form of slavery once and for all.

We are also marking up the Crimea Annexation Nonrecognition Act. This bill clearly states that America will not recognize Russian sovereignty over Crimea.

Doing so would condone Russia's belligerent behavior toward its neighbors. Vladimir Putin needs to understand that we will not tolerate this kind of aggression in Crimea or anywhere else in the world.

And that is also why today's resolution condemning the assassination of Boris Nemtsov is also important. We cannot be silent when political opponents are targeted for supporting democratic reforms.

I was proud to introduce this resolution with Chairman Engel because Putin needs to know that both Democrats and Republicans will call out and condemn his authoritarian ways.

And finally, we must continue to stand united in our fight against Islamist terrorism. The terror attack in Nairobi, Kenya, on January the 15th that killed 21 people including Jason Spindler, a fellow Texan, was a painful reminder that our fight against terrorism is a global struggle.

Our resolution condemns this attack and reaffirms our commitment to eradicating this evil.

I look forward to passing these bills out of committee with bipartisan support.

And, finally, Mr. Chairman, on the floor and in the halls of Congress there has been much discussion recently about anti-Semitism. I want to thank you for your leadership on this issue and I look forward to continuing to work with you on measures that support our close ally, Israel, and denounce anti-Semitism wherever it may be.

And with that, I yield back the balance of my time.

Chairman ENGEL. Thank you, Mr. McCaul.

Are there any other members seeking recognition?

Mr. CONNOLLY. Mr. Chairman?

Chairman ENGEL. Yes, Mr. Connolly.

Mr. CONNOLLY. I thank the chair and the ranking member. I want to thank them both for putting together this bipartisan package of five bills for our consideration today.

These measures condemn terrorist attacks, strengthen U.S. diplomacy, condemn Russia's violations of human rights and territorial sovereignty, and bolster U.S. efforts to reduce global human trafficking, the scourge of our time.

In particular, Mr. Chairman, I would like to thank you and the ranking member for including in this markup H.R. 596, the Crimea Annexation Nonrecognition Act, which I introduced with my good friend and Republican colleague, Representative Steve Chabot.

This bill states that it is the policy of the United States not to recognize the Russian Federation's claim of sovereignty over Crimea, its airspace, or its territorial waters.

Furthermore, this bill prohibits the U.S. Government from taking any action that implies recognition of Russian sovereignty over Crimea.

It has been the longstanding policy of the United States to not recognize territorial changes effected by force as dictated by the long-ago Stimson Doctrine established in 1932 by then-Secretary of State Henry Stimson.

The matter of rejecting the forcible and illegal attack on sovereign territory is so important we should be satisfied with nothing less than absolute clarity about our position, which is one that supports Ukraine sovereignty over its own territory in Crimea.

Failure to stand up, as Mr. McCaul just said, to Putin's illegal annexation of Crimea sets a dangerous and irrevocable precedent. Crimea was Russia's original violation in Ukraine and we have limited credibility objecting to Russia's subsequent invasion of the Luhansk and Donetsk if we do not take a stand in Crimea.

Russian occupation of Crimea has inflicted great harm within the Ukraine, throughout former Soviet occupied territories, and beyond.

What has happened in Ukraine—Russia's forcible and illegal annexation of Crimea, its invasion of Eastern Ukraine, and continued occupation in Crimea, Luhansk and Donetsk, has precipitated an international crisis and the resulting conflict has claimed more than 10,000 lives.

Russia has subjected Crimeans who refuse Russian citizenship to discrimination in accessing education, health care, and employ-

ment, and Russian authorities have attacked travel rights and the free press.

Acquiescence on the part of the United States threatens the security of all sovereign nations. Russia's forcible and illegal annexation of Crimea has sent shock waves throughout the former Soviet occupied territories, many of whom are now NATO allies, including the Baltic States.

After the Welles Declaration in June 1940, the U.S. refused to recognize the Soviet Union's de facto or de jure sovereignty over the Baltics during the Soviet Union's 50 years of illegal occupation.

The Baltic Republics eventually received their independence and they are now reliable NATO allies, in part because of our steadfastness.

We first introduced this bill in the wake of Russia's forcible and illegal annexation in 2014. This committee previously passed this legislation in the 113th Congress.

I inserted similar language into the Fiscal Year 2016 National Defense Authorization Act in order to prohibit the use of defense funds in a manner that recognizes Russian sovereignty over Crimea. That is to say that we did not.

That language has remained in the NDAA, I am grateful to say, every year since. I have also successfully authored an amendment to Stand For Ukraine Act, which would create only one condition under which the president can relax Crimea-related sanctions—the restoration of Ukraine sovereignty.

The United States must lead the way in refusing to recognize or legitimize Russia's illegal and forcible annexation in Crimea. That is why both Mr. Chabot and I are glad to offer this bill, which expresses the will of Congress as a loud and declarative voice for sovereignty and freedom and I urge my colleagues to support it.

And, again, I thank the chair and ranking member for including it in today's markup. I yield back.

Chairman ENGEL. Thank you very much, Mr. Connolly.

Mr. SMITH.

Mr. SMITH. Thank you very much, Mr. Chairman.

Chairman, I strongly support your resolution, H. Res. 156, calling for accountability and justice for the assassination of Boris Nemtsov, a Russian patriot killed in 2015, a great defender of democracy in his home country of Russia.

Last July, I had the privilege of leading the United States delegation to the OSCE Parliamentary Assembly in Berlin and I actually chaired the public event that you reference in your resolution, the July 8th public event, and we featured Hanna Nemtsova, Boris Nemtsov's daughter, who was absolutely compelling and brave and full of courage.

Boris's friend and colleague, Vladimir Kara-Murza, who serves as chairman of the board of trustees for the Boris Nemtsov Foundation for Freedom, and Vadim Prokhorov, who is a lawyer for the Nemtsov family.

I believe that this resolution is a timely followup to that OSCE effort because we have been calling on the administration to do more and I think the fact that you articulate the concern and the need, frankly, to do some better reporting and to hold those respon-



sible besides the five low-level individuals who have been tried—who ordered the hit.

It was an assassination, and it seems to me that it is time, frankly, to really impose Magnitsky sanctions on those who are directly responsible for this. But we need that information. We need our government to redouble down. So thank you for that resolution.

Second, I do want to thank you for marking up H.R. 295, the End Banking for Human Traffickers Act of 2019. This is authored, of course, by my good friend and colleague, Mr. Fitzpatrick.

This bill will help ensure that human traffickers find trafficking even more unprofitable because they will be curbed in their financial work that they do. They often use banks. This helps to increase that net to catch these people.

We have been making strides, Mr. Chairman, in this direction. For example, last Congress the Frederick Douglass Trafficking Victims Prevention and Protection Reauthorization Act, which I authored along with my friend and colleague, Karen Bass, the prime Democratic co-sponsor, was signed into law on January 8th, and among its many provisions, it added the secretary of the Treasury to the President's Inter-Agency Task Force to monitor and combat trafficking in persons.

H.R. 295 calls on the task force to evaluate the anti-money laundering efforts of the U.S. Government and U.S. financial institutions to see if we are doing enough, and I do not think we are, to recognize and act against financial movements to signal red flags that human trafficking is occurring.

The task force will consult with trafficking survivors and the financial industry representatives who have been pioneering anti-trafficking efforts in their best practices.

So, again, I want to thank you for all of these bills. I think they are all excellent pieces of legislation and I especially want to thank Mr. Fitzpatrick for his leadership on combatting the scourge of human trafficking.

Chairman ENGEL. Thank you, Mr. Smith.

Is there anyone else who seeks recognition?

Mr. CHABOT. Mr. Chairman? Mr. Chairman?

Chairman ENGEL. Mr. Chabot.

Mr. CHABOT. Thank you, Mr. Chairman. Move to strike the last word.

Mr. Chairman, I want to thank you for holding this markup today, and I want to thank you for this slate of five excellent bipartisan bills.

First, Ukraine—I am honored to be the lead Republican co-sponsor of H.R. 596, Mr. Connolly's Crimean Annexation Nonrecognition Act, and I want to thank him for his hard work on this important legislation.

We have been working together on this since the bully Putin first acted on Crimea. I know a number of members of this committee have done so and I think it is critical that we continue to do so. So I want to thank Mr. Connolly for his hard work on this.

Passage of this bill would cement firmly in place the policy that the United States will not recognize Putin's bogus claims over Crimea and will prohibit any part of our government from taking any

action that would imply our recognition of Russian sovereignty over the peninsula.

It is vitally important that we support a democratic and unified Ukraine by not giving in to Putin's thuggish behavior and that behavior continues.

For example, in November, Russian vessels blockaded the Kerch Strait, the entrance to the Sea of Azov, and illegally seized Ukrainian naval vessels.

By these and other actions, Putin is seeking to strangle Ukraine's trade and in all likelihood annex more of it. We cannot let that happen. The world cannot stand by as it did previously when Putin annexed Crimea.

Unfortunately, Putin's gangster ways are not confined to his foreign policy. That is why we are considering H. Res. 156, which I am also a co-sponsor of. This resolution calls for justice for Boris Nemtsov, who, as was mentioned, was murdered in cold blood near the Kremlin on February 25th of 2015.

For those who do not know, Mr. Nemtsov was a leading opposition figure, outspoken Putin critic, and the former first deputy prime minister of Russia and was in all likelihood—we do not know for absolutely sure—but in all likelihood was executed at the direction of Putin.

The Russian government must do a thorough investigation to uncover the truth behind Mr. Nemtsov—that we should not let this rest.

I also want to turn briefly to a couple of other bills we have. The terrorist attack on Kenya earlier this year is yet another example of the scourge of radical terrorism and we must continue to fight against that every time it rears its ugly head.

That is why I am a co-sponsor of H. Res. 75. And finally, I want to thank Ranking Member McCaul for his leadership on the critical issue of Cybersecurity.

As a co-sponsor of the Cyber Diplomacy Act, I think it is necessary that we work with our like-minded allies to ensure that the internet remains a place of robust debate and access to uncensored information.

This legislation provides the State Department tools and direction to help accomplish this important priority, and I want to echo the words that our ranking member mentioned before—Mr. McCaul.

I completely agree with him that there is absolutely no place for anti-Semitism in this country, on this globe, or in this committee. I have been on this committee for a long time—23 years—and we have always been bipartisan on that issue. I would hope that would continue.

Israel is a strong ally of the United States. The Jewish people have been for a long time and will continue to be, whether it is as a nation or whether as a people, and there is absolutely no room for anti-Semitism.

And I think that we should work on that in a bipartisan manner, and it always has been that way. I hope it will be in the future. There is absolutely no place for anti-Semitism.

Thank you, Mr. Chairman.

Chairman ENGEL. Thank you very much, Mr. Chabot.

Mr. MALINOWSKI.

Mr. MALINOWSKI. Thank you. Thank you so much, Chairman Engel, Ranking Member McCaul.

I wanted to say a few words in particular about the resolution regarding Boris Nemtsov and to explain the two small amendments that I will be offering today.

First of all, thank you for introducing this resolution to help us remember this very good man and to put the Putin regime on notice that we are not going to forget what happened and who is responsible.

If you read the resolution, you will see that one of the central villains in this terrible story is Ramzan Kadyrov, the strong man who rules and has ruled Chechnya with an iron hand for many, many years.

Even the flawed Russian investigation of the murder of Mr. Nemtsov determined that the murder was carried out by members of an elite battalion loyal to Kadyrov.

Kadyrov publicly praised the gunmen. Previously, he had publicly called for the death of Nemtsov. One of the chief suspects is still living at large in Chechnya under Kadyrov's protection.

Kadyrov has also, over the years, been credibly accused of murdering human rights activists, journalists. He has ordered his police forces to round up and torture gay men and women in Chechnya. He has ordered the assassination of his critics living in other countries, in Europe, and in the Middle East.

In 2017, the U.S. Government put Mr. Kadyrov on the Global Magnitsky sanctions list, which means that his business activities overseas involving any sort of transactions through international banks should be blocked.

In reality, though, Mr. Kadyrov has repeatedly shown himself outside of Russia, particularly in Persian Gulf countries such as the UAE and Saudi Arabia.

His hobby is horse racing. He spends millions of dollars purchasing race horses, winning races around the world, again, particularly in the Middle East.

He is blocked in Europe. What my first amendment does is simply to urge the administration to prioritize sanctions-enforcement with respect to Ramzan Kadyrov, to investigate his business activities and that of entities he may control outside of the Russian federation and to determine whether any of them might implicate the sanctions that we have imposed.

The second amendment ensures that the resolution includes an additional key suspect in Mr. Nemtsov's murder, Adam Delimkhanov, who is a notorious associate and relative of Ramzan Kadyrov.

Delimkhanov is a member of the Russian State Duma where he has abused his immunity to shield himself from accountability for a range of human rights abuses.

He has been identified by multiple independent sources as one of the organizers of Mr. Nemtsov's murder. So this amendment would add his name to the list of suspects in two clauses of the resolution's preamble.

I ask my colleagues to support both of these amendments. Thank you very much.

Chairman ENGEL. Thank you, Mr. Malinowski.

Mr. FITZPATRICK.

Mr. FITZPATRICK. Thank you, Mr. Chairman.

Chairman, Ranking Member, I really do appreciate your considering of H.R. 295. As an FBI agent, one of the most horrific crimes that we were called upon to investigate was human trafficking, and human trafficking continues to devastate millions of lives around the world.

And this criminal conduct may seem a distant problem but it is far from it. It exists right in all of our back yards, in every single congressional district in this country, in all of our communities, and at times it is right in front of us and we do not even know it exists.

My legislation, H.R. 295, the End Banking of Human Traffickers Act, is one step we can take to end the suffering caused by human trafficking.

Traffickers are not hiding their illegal profits under a mattress or burying them in their back yard. They use our very sophisticated global financial system to launder their illicit funds through banks, credit card companies, and money transfer companies, which are all used by traffickers to facilitate their business and to perpetuate their exploitation of victims.

The scale of profits from this illicit trade is really staggering. The International Labor Organization estimates that over \$150 billion in illegal profits are made from forced labor each year, and \$99 billion are earned through the exploitation of victims of sexual exploitation, making human trafficking the third most lucrative criminal enterprise on this planet.

The perpetrators of this exploitation play on the defenseless in our society, including young children. Cutting off their access to the banking system is a critical aspect both from the investigative standpoint, and the legislative standpoint and I am proud to push this bipartisan bill with my friend and colleague, Congressman Keating, to continue working to end this horror once and for all.

And I thank my colleagues both on and off this committee for their support, many of whom have joined this effort. I also want to thank Congressman Chris Smith from New Jersey, who has made it one of his top priorities to advance this mission.

This legislation directs Federal banking regulators to work with law enforcement and financial institutions to combat the use of the financial system for human trafficking.

The bill further increases collaboration between law enforcement and experts in financial crimes by adding financial intelligence and regulatory officers to the President's Inter-Agency Task Force to monitor and combat trafficking in persons and requires the task force to develop recommendations for Congress and regulators that would strengthen anti-money laundering programs to better target human trafficking.

Moreover, this bill allows advocates of human trafficking victims to serve as stakeholders and to provide feedback to the U.S. Treasury and, additionally, clarifies that banks not restrict trafficker victims' access to bank accounts.

I urge ever Member of Congress, especially those on this committee, to support this legislation, which passed both the committee and the House last Congress with broad bipartisan support.

We must do everything possible to put an end to human trafficking and this legislation is a very important step along that path.

Mr. Chairman, I yield back.

Chairman ENGEL. Thank you, Mr. Fitzpatrick.

Is there anyone else who seeks recognition?

OK. Hearing no further requests for recognition, then without objection the committee will proceed to consider the noticed items en bloc. A reporting quorum is present.

Without objection, the question occurs on the measures en bloc as amended.

All those in favor, say aye.

All those opposed, no.

In the opinion of the chair, the ayes have it.

The measures considered en bloc are agreed to and without objection each measure in the en bloc is ordered favorably reported as amended and each amendment to each bill shall be reported as a single amendment in the nature of a substitute.

Without objection, staff is authorized to make any technical and conforming changes and the chair is authorized to seek House consideration under suspension of the rules.

This concludes——

Mr. MCCAUL. Mr. Chairman?

Chairman ENGEL. Yes, Mr. McCaul.

Mr. MCCAUL. Pursuant to House rules, I request that members have the opportunity to submit views for any committee report that may be produced on any of today's measures.

Chairman ENGEL. Obviously, there is no objection to that and I thank Ranking Member McCaul and all of the committee members for their contribution and assistance with today's markup.

The committee stands adjourned.

[Whereupon, at 10:37 a.m., the committee was adjourned.]

**FULL COMMITTEE MARKUP NOTICE  
COMMITTEE ON FOREIGN AFFAIRS  
U.S. HOUSE OF REPRESENTATIVES  
WASHINGTON, DC 20515-6128**

**Eliot L. Engel (D-NY), Chairman**

March 7, 2019

**TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS**

You are respectfully requested to attend an OPEN markup of the Committee on Foreign Affairs to be held in Room 2172 of the Rayburn House Office Building (and available live on the Committee website at <https://foreignaffairs.house.gov/>):

**DATE:** Thursday, March 7, 2019

**TIME:** 10:00 a.m.

**MARKUP OF:** H.Res. 75, Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi, Kenya

H.R. 739, Cyber Diplomacy Act of 2019

H.Res. 156, Calling for accountability and justice for the assassination of Boris Nemtsov

H.R. 596, Crimea Annexation Non-recognition Act

H.R. 295, End Banking for Human Traffickers Act of 2019

**By Direction of the Chairman**

The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202/225-5021 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.

**COMMITTEE ON FOREIGN AFFAIRS**  
**MINUTES OF FULL COMMITTEE MARKUP**

Day Thursday Date 03/07/19 Room 2172 RHOB

Starting Time 10:05 a.m. Ending Time 10:37 a.m.

Recesses 0 ( to ) ( to ) ( to ) ( to ) ( to ) ( to )

Presiding Member(s)  
 Chairman Ellot Engel

Check all of the following that apply:

Open Session       Electronically Recorded (taped)   
 Executive (closed) Session       Stenographic Record   
 Televised

**BILLS FOR MARKUP: (Include bill number(s) and title(s) of legislation.)**

H.Res. 75, Strongly condemning the January 2019 terrorist attack on the 14 Riverside  
 Complex in Nairobi, Kenya  
 H.R. 709, Cyber Diplomacy Act of 2019  
 H.Res. 156, Calling for accountability and justice for the assassination of Boris Nemtsov  
 H.R. 296, Cyber Assassination Non-Interference Act  
 H.R. 295, End Banishing for Human Traffickers Act of 2019

**COMMITTEE MEMBERS PRESENT:**  
*See attached.*

**NON-COMMITTEE MEMBERS PRESENT:**  
*N/A*

**STATEMENTS FOR THE RECORD: (List any statements submitted for the record.)**  
*SFR\_Castro*

**ACTIONS TAKEN DURING THE MARKUP: (Attach copies of legislation and amendments.)**  
*The measures considered en bloc were agreed to by voice vote.*

**RECORDED VOTES TAKEN (FOR MARKUP): (Attach final vote tally sheet listing each member.)**

Subject	Yeas	Nays	Present	Not Voting
<i>N/A</i>	<i>N/A</i>	<i>N/A</i>	<i>N/A</i>	<i>N/A</i>

**TIME SCHEDULED TO RECONVENE** \_\_\_\_\_  
 or  
**TIME ADJOURNED** 10:37 a.m.

  
 Full Committee Hearing Coordinator

**HOUSE COMMITTEE ON FOREIGN AFFAIRS**  
*FULL COMMITTEE MARKUP*

<i>PRESENT</i>	<i>MEMBER</i>
X	Eliot L. Engel, NY
X	Brad Sherman, CA
	Gregory W. Meeks, NY
X	Albio Sires, NJ
X	Gerald E. Connolly, VA
	Theodore E. Deutch, FL
	Karen Bass, CA
	William Keating, MA
	David Cicilline, RI
	Ami Bera, CA
X	Joaquin Castro, TX
X	Dina Titus, NV
	Adriano Espaillat, NY
X	Ted Lieu, CA
X	Susan Wild, PA
X	Dean Phillips, MN
X	Ilhan Omar, MN
X	Colin Allred, TX
X	Andy Levin, MI
X	Abigail Spanberger, VA
X	Chrissy Houlahan, PA
X	Tom Malinowski, NJ
	David Trone, MD
X	Jim Costa, CA
X	Juan Vargas, CA
X	Vicente Gonzalez, TX

<i>PRESENT</i>	<i>MEMBER</i>
X	Michael T. McCaul, TX
X	Christopher H. Smith, NJ
X	Steve Chabot, OH
	Joe Wilson, SC
X	Scott Perry, PA
X	Ted Yoho, FL
X	Adam Kinzinger, IL
X	Lee Zeldin, NY
	James Sensenbrenner, Jr., WI
X	Ann Wagner, MO
X	Brian J. Mast, FL
X	Francis Rooney, FL
X	Brian K. Fitzpatrick, PA
X	John Curtis, UT
X	Ken Buck, CO
X	Ron Wright, TX
X	Guy Reschenthaler, PA
X	Tim Burchett, TN
X	Greg Pence, IN
X	Steve Watkins, KS
X	Michael Guest, MS



**Statement for the Record from Representative Joaquin Castro**  
Markup of Various Measures  
March 7, 2019

Thank you, Chairman Engel and Ranking Member McCaul, for your leadership on this committee.

I want to congratulate all the members whose bills are being considered here today.

These measures cover a wide range of challenges we face around the world.

These challenges include terrorism, assassination, cyber diplomacy, human trafficking, international aggression—all of which fall within this Committee's jurisdiction.

I am happy to support each of the measures brought today that will address these important issues.

I'd like to speak about just a few.

Firstly, we are acutely aware of the many challenges that cyber space presents to our national security.

Our adversaries have actively used the domain to meddle in our democracy, steal data, and much more.

But there are also opportunities to strengthen diplomacy to address these challenges and in turn strengthen our alliances abroad.

It is only natural that we should complement our cyber defenses with cyber diplomacy.

This bipartisan bill sets forth a U.S. international cyberspace policy that promotes an open, interoperable, reliable, unfettered, and secure Internet.

It also lays out a model that promotes human rights, democracy, and the rule of law, while respecting privacy and guarding against deception, fraud, and theft.

The State Department will have the lead in setting cyber diplomacy policy with the establishment of an Office of Cyber Issues.

This legislation will improve our nation's ability to conduct cyber diplomacy within a policy framework.

I'm happy to support this important measure that will strengthen U.S. national security and diplomacy abroad.

We've seen Putin's growing aggression and disregard for international law with his annexation of Crimea in 2014, hacking of our democracy in 2016, 2018 and now likely 2020, and repeated murders of opposition figures within Russia's society.

I'd like to thank Mr. Chabot for sending Congress' disapproval message of the annexation of Crimea, and introducing a resolution that will prohibit any federal department from recognizing Russia as exercising sovereignty over Crimea.

It only makes logical sense that the U.S. government should not be in the business of rewarding such aggression.

This resolution makes the correct statement of policy that the U.S. government will not recognize Russia's annexation of Crimea and I'm proud to support it.

I would also like to voice my support for this resolution that demands justice for Boris Nemtsov, a Russian statesman who was assassinated in February of 2015.

Mr. Nemtsov had an unwavering commitment to the ideals of democracy, freedom, and the rule of law, vocally opposing the authoritarianism espoused by Vladimir Putin.

Ultimately becoming victim to state-sponsored murder, this is not an isolated event.

From Saudi Arabia, to North Korea, and other places in between, we continue to see authoritarians target people who dare to critique their policies and regimes.

We have a President who would rather nurture relationships with authoritarian thugs than repudiate their strong man tactics.

This resolution allows Congress to send a message loud and clear.

Brutal authoritarian regimes that target their political critics are a threat to democracy and rule of law globally.

Lastly, human traffickers are preying on vulnerable populations throughout the world.

We must do everything in our power to combat an issue that in many cases amounts to modern day slavery.

One facet of that is clamping down on financial streams that breathe life into these networks.

This legislation does just that, and I'm proud to support it.

I'm glad to support all the measures before us today.

Thank you again Mr. Chairman for your leadership, and to my colleagues for introducing these important measures.

**03/07/2019 House Foreign Affairs Committee Markup Summary**

By unanimous consent, the Chair called up the following measures and amendments, previously provided to Members, to be considered *en bloc*:

- (1) H.Res. 75, Strongly condemning the January 2019 terrorist attack on the 14 Riverside Complex in Nairobi Kenya, (Engel)
- (2) H.R. 739, Cyber Diplomacy Act of 2019, (McCaul)
  - McCaul Amendment #14
- (3) H.Res. 156, Calling for accountability and justice for the assassination of Boris Nemtsov (Engel)
  - Malinowski Amendment #11
  - Malinowski Amendment #A1
- (4) H.R. 596, Crimea Annexation Non-recognition Act (Connolly)
  - Connolly, an amendment in the nature of a substitute to H.R. 596
- (5) H.R. 295, End Banking for Human Traffickers Act of 2019 (Fitzpatrick)
  - Engel, an amendment in the nature of a substitute to H.R. 295

The measures considered *en bloc* were agreed to by voice vote.

By unanimous consent, the measures were ordered favorably reported, as amended, to the House, and the Chairman was authorized to seek House consideration under suspension of the rules.

The Committee adjourned.