Barack Obama—and visited a number of African countries, in particular Kenya, we were there to look at the rising population of small- and medium-sized entrepreneurs, young millennials, and others who were eager to engage in business.

The African Growth and Opportunity Act will be a pathway for sub-Saharan African countries in that area that will create the pathway for trade for the goods of those produced on the continent.

Peace and the economy go together. If we have an economic engine partnership with the United States, looking at good quality investment, and if we have the work of the Millennium Challenge to challenge countries to become more democratic, to open the doors of opportunity, to have a better fiscal system, and to be a real partner in these improvements, that is a real African policy.

So I rise to support the underlying bill, H.R. 3445. I rise to support it because it is an advancement to the work that has been done over the years by the United States Congress and the many partners that we have had.

I am a student of Africa, having gone to school in Accra and Kumasi in Ghana and, of course, in Lagos and Ibadan in Nigeria. I have traveled often, and I understand the ingenuity, the eagerness, and the commitment to democratic principles and, of course, the opportunities for their young generation.

So I rise today to support the bill. I thank the sponsors for this very excellent legislation. It is good work.

Mr. Speaker, I don't know if it is appropriate, but I ask unanimous consent to cosponsor the legislation at this time.

The SPEAKER pro tempore. The gentlewoman's request to be added as a cosponsor cannot be entertained at this point on this bill.

Mr. SIRES. Mr. Speaker, I yield back the balance of my time.

Mr. ROYCE of California. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I will sum up here. What this bill does is unlock a greater potential for AGOA, for the African Growth and Opportunity Act, so communities in Africa can strengthen their own economies and become U.S. trade partners rather than aid recipients. It also enhances the impact of MCC by accelerating regional economic integration trade.

It is good for American taxpayers. It is certainly good for job creators in the United States. It is good for our national security. It is good for Africa—for the people of Africa.

I think this legislation is the product of more than 2 years of negotiations. It enjoys very broad support. As I say, it doesn't cost the taxpayers anything.

I really want to thank some of the Members who worked hard on this. I thank Representative KAREN BASS for her good work, Congresswoman SHEILA JACKSON LEE, Ranking Member ENGEL, and Representative CHRIS SMITH; Senators CORKER, CARDIN, ISAKSON, and COONS. I thank them for their help on my measure here today and for their continued commitment to reducing poverty through market-based economic growth.

Mr. Speaker, I yield back the balance of my time.

Mr. SMITH of New Jersey. Mr. Speaker, I rise today in support of H.R. 3445, the African Growth and Opportunity Act and Millennium Challenge Act Modernization Act.

I am an original cosponsor of H.R. 3445, and as Chairman of the House Foreign Affairs Africa subcommittee, I want to applaud Chairman ROYCE, Ranking Member ELLIOT ENGEL, and the Ranking Member of my subcommittee, KAREN BASS, for their commitment to Africa and to enhancing trade, and all the benefits in terms of closer relationships that flow from trade, between the people of the United States and the people of Africa.

The original AGOA Act of 2000 has been called a ''cornerstone'' of our trade policy toward the continent, and it has served us well. Over the years, however, our subcommittee has had numerous hearings—not to mention meetings with African heads of state and ambassadors—on AGOA, increasing exports to Africa, and on cultivating the-rule-of-law reforms necessary to attract business and investment to Africa. In past Congresses I introduced the Increasing American Jobs Through Greater Exports to Africa Act. It has become apparent that, as well as AGOA has served us, there is room for improvement and innovation.

H.R. 3445 marks a step toward that, by emphasizing capacity building and training and encouraging entrepreneurship in Africa. Importantly, it acknowledges that the world has changed since 2000, and that Africa has been targeted by radical extremists such as Boko Haram and al-Shabaab. Recognizing that we now live in a post-2001 world, H.R. 3445 fosters compliance with our counterterrorism initiatives by African businesses and institutions.

Africa, and much of the developing world, has also benefitted from the Millennium Challenge Corporation since passage of the Millennium Challenge Act of 2003. MCC is a critical partner, for example, in our Global Food Security strategy, which fosters agriculture-led economic development.

Though MCC has played a key role, there are also room for improvements. Sometimes during the country selection process, narratives about a country become set, and there is not a fresh appraisal of evidence regarding improvements, or backsliding, in the conditions of that country.

I'd like to thank Chairman ROYCE for working to ensure that MCC remains a vehicle focused on assisting countries with development, and does not become diverted from its original mission.

I urge my colleagues to join me in support of H.R. 3445, the African Growth and Opportunity Act and Millennium Challenge Act Modernization Act.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from California (Mr. ROYCE) that the House suspend the rules and pass the bill, H.R. 3445, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

CYBER DIPLOMACY ACT OF 2017

Mr. ROYCE of California. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3776) to support United States international cyber diplomacy, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3776

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cyber Diplomacy Act of 2017''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) The stated goal of the United States International Strategy for Cyberspace, launched on May 16, 2011, is to ''work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation . . . in which norms of responsible behavior guide States' actions, sustain partnerships, and support the rule of law in cyberspace.''.

(2) The Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, established by the United Nations General Assembly, concluded in its June 24, 2013, report ''that State sovereignty and the international norms and principles that flow from it apply to States' conduct of [information and communications technology or ICT] related activities and to their jurisdiction over ICT infrastructure with their territory.''.

(3) On January 13, 2015, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan proposed a troubling international code of conduct for information security which defines responsible State behavior in cyberspace to include ''curbing the dissemination of information'' and the ''right to independent control of information and communications technology'' when a country's political security is threatened.

(4) The July 22, 2015, GGE consensus report found that, ''norms of responsible State behavior can reduce risks to international peace, security and stability.''.

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

(6) At the Antalya Summit from November 15–16, 2015, the Group of 20 (G20) Leaders' Communique affirmed the applicability of international law to State behavior in cyberspace, called on States to refrain from cyber-enabled theft of intellectual property for commercial gain, and endorsed the view that all States should abide by norms of responsible behavior.

(7) The March 2016 Department of State International Cyberspace Policy Strategy noted that, ''the Department of State anticipates a continued increase and expansion of our cyber-focused diplomatic efforts for the foreseeable future.''.

(8) On December 1, 2016, the Commission on Enhancing National Cybersecurity established

within the Department of Commerce recommended ''the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices.''.

(9) The 2017 Group of 7 (G7) Declaration on Responsible States Behavior in Cyberspace recognized on April 11, 2017, ''the urgent necessity of increased international cooperation to promote security and stability in cyberspace . . . consisting of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime'' and reaffirmed ''that the same rights that people have offline must also be protected online.''.

(10) In testimony before the Select Committee on Intelligence of the Senate on May 11, 2017, the Director of National Intelligence identified six cyber threat actors, including Russia for ''efforts to influence the 2016 US election''; China, for ''actively targeting the US Government, its allies, and US companies for cyber espionage''; Iran for ''leverage[ing] cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats''; North Korea for ''previously conduct[ing] cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014''; terrorists, who ''use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations''; and criminals who ''are also developing and using sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activities''.

(11) On May 11, 2017, President Trump issued Presidential Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Infrastructure which designated the Secretary of State to lead an interagency effort to develop strategic options for the President to deter adversaries from cyber threats and an engagement strategy for international cooperation in cybersecurity, noting that ''the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners'' toward maintaining ''the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against deception, fraud, and theft.''.

SEC. 3. UNITED STATES INTERNATIONAL CYBERSPACE POLICY.

(a) IN GENERAL.—Congress declares that it is the policy of the United States to work internationally with allies and other partners to promote an open, interoperable, reliable, unfettered, and secure internet governed by the multistakeholder model which promotes human rights, democracy, and rule of law, including freedom of expression, innovation, communication, and economic prosperity, while respecting privacy and guarding against deception, fraud, and theft.

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

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

(2) Clarifying that countries that fall victim to malicious cyber activities have the right to take proportionate countermeasures under international law, provided such measures do not violate a fundamental human right or peremptory norm.

(3) Reducing and limiting the risk of escalation and retaliation in cyberspace, such as massive denial-of-service attacks, damage to critical infrastructure, or other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public.

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

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

(A) Countries should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

(B) Countries should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

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

(D) Countries should not conduct or knowingly support ICT activity that, contrary to international law, intentionally damages or otherwise impairs the use and operation of critical infrastructure, and should take appropriate measures to protect their critical infrastructure from ICT threats.

(E) Countries should not conduct or knowingly support malicious international activity that, contrary to international law, harms the information systems of authorized emergency response teams (sometimes known as ''computer emergency response teams'' or ''cybersecurity incident response teams'') or related private sector companies of another country.

(F) Countries should identify economic drivers and incentives to promote securely-designed ICT products and to develop policy and legal frameworks to promote the development of secure internet architecture.

(G) Countries should respond to appropriate requests for assistance to mitigate malicious ICT activity aimed at the critical infrastructure of another country emanating from their territory.

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

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

SEC. 4. DEPARTMENT OF STATE RESPONSIBILITIES.

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

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

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

''(g) OFFICE OF CYBER ISSUES.—

''(1) IN GENERAL.—There is established an Office of Cyber Issues (in this subsection referred to as the 'Office'). The head of the Office shall have the rank and status of ambassador and be appointed by the President, by and with the advice and consent of the Senate.

''(2) DUTIES.—

''(A) IN GENERAL.—The head of the Office shall perform such duties and exercise such powers as the Secretary of State shall prescribe, including implementing the policy of the United States described in section 3 of the Cyber Diplomacy Act of 2017.

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

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

''(ii) lead the Department of State's diplomatic cyberspace efforts generally, including relating to international cybersecurity, internet access, internet freedom, digital economy, cybercrime, deterrence and international responses to cyber threats;

''(iii) promote an open, interoperable, reliable, unfettered, and secure information and communications technology infrastructure globally;

''(iv) represent the Secretary of State in interagency efforts to develop and advance the United States international cyberspace policy;

''(v) coordinate within the Department of State and with other components of the United States Government cyberspace efforts and other relevant functions, including countering terrorists' use of cyberspace; and

''(vi) act as liaison to public and private sector entities on relevant cyberspace issues.

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

''(A) cybersecurity and other relevant cyber issues; and

''(B) international diplomacy.

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

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

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

''(B) the head of the Office from being elevated to an Assistant Secretary, if such an Assistant Secretary position does not increase the number of Assistant Secretary positions at the Department above the number authorized under subsection (c)(1).''.

(b) SENSE OF CONGRESS.—It is the sense of Congress that the Office of Cyber Issues established under section 1(g) of the State Department Basic Authorities Act of 1956 (as amended by subsection (a) of this section) should be a Bureau of the Department of State headed by an Assistant Secretary, subject to the rule of construction specified in paragraph (5)(B) of such section 1(g).

(c) UNITED NATIONS.—The Permanent Representative of the United States to the United Nations shall use the voice, vote, and influence of the United States to oppose any measure that is inconsistent with the United States international cyberspace policy described in section 3.

SEC. 5. INTERNATIONAL CYBERSPACE EXECUTIVE ARRANGEMENTS.

(a) IN GENERAL.—The President is encouraged to enter into executive arrangements with foreign governments that support the United States international cyberspace policy described in section 3.

(b) TRANSMISSION TO CONGRESS.—The text of any executive arrangement (including the text of any oral arrangement, which shall be reduced to writing) entered into by the United States under subsection (a) shall be transmitted to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate not later than five days after such arrangement is signed or otherwise agreed to, together with an explanation of such arrangement, its purpose, how such arrangement is consistent with the United States international cyberspace policy described in section 3, and how such arrangement will be implemented.

(c) STATUS REPORT.—Not later than one year after the text of an executive arrangement is transmitted to Congress pursuant to subsection (b) and annually thereafter for seven years, or

until such an arrangement has been discontinued, the President shall report to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate on the status of such arrangement, including an evidence-based assessment of whether all parties to such arrangement have fulfilled their commitments under such arrangement and if not, what steps the United States has taken or plans to take to ensure all such commitments are fulfilled, whether the stated purpose of such arrangement is being achieved, and whether such arrangement positively impacts building of cyber norms internationally. Each such report shall include metrics to support its findings.

(d) EXISTING EXECUTIVE ARRANGEMENTS.—Not later than 60 days after the date of the enactment of this Act, the President shall satisfy the requirements of subsection (c) for the following executive arrangements already in effect:

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

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

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

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

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

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

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

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

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

(10) Any other similar bilateral or multilateral arrangement announced before the date of the enactment of this Act.

SEC. 6. INTERNATIONAL STRATEGY FOR CYBERSPACE.

(a) STRATEGY REQUIRED.—Not later than one year after the date of the enactment of this Act, the Secretary of State, in coordination with the heads of other relevant Federal departments and agencies, shall produce a strategy relating to United States international policy with regard to cyberspace.

(b) ELEMENTS.—The strategy required under subsection (a) shall include the following:

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

(2) A plan of action to guide the diplomacy of the Department of State with regard to foreign countries, including conducting bilateral and multilateral activities to develop the norms of responsible international behavior in cyberspace, and status review of existing efforts in multilateral fora to obtain agreements on international norms in cyberspace.

(3) A review of alternative concepts with regard to international norms in cyberspace offered by foreign countries.

(4) A detailed description of new and evolving threats to United States national security in cyberspace from foreign countries, State-sponsored actors, and private actors to Federal and private sector infrastructure of the United States, intellectual property in the United States, and the privacy of citizens of the United States.

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

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

(7) A clarification of the applicability of international laws and norms, including the law of armed conflict, to the use of ICT.

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

(9) A plan of action to guide the diplomacy of the Department of State with regard to existing mutual defense agreements, including the inclusion in such agreements of information relating to the applicability of malicious cyber activities in triggering mutual defense obligations.

(c) FORM OF STRATEGY.—

(1) PUBLIC AVAILABILITY.—The strategy required under subsection (a) shall be available to the public in unclassified form, including through publication in the Federal Register.

(2) CLASSIFIED ANNEX.—

(A) IN GENERAL.—If the Secretary of State determines that such is appropriate, the strategy required under subsection (a) may include a classified annex consistent with United States national security interests.

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

(d) BRIEFING.—Not later than 30 days after the production of the strategy required under subsection (a), the Secretary of State shall brief the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate on such strategy, including any material contained in a classified annex.

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

(1) not later than 90 days after there has been any material change to United States policy as described in such strategy; and

(2) not later than one year after each inauguration of a new President.

(f) PREEXISTING REQUIREMENT.—Upon the production and publication of the report required under section 3(c) of the Presidential Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure on May 11, 2017, such report shall be considered as satisfying the requirement under subsection (a) of this section.

SEC. 7. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES.

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

''(h)(1) The report required by subsection (d) shall include an assessment of freedom of expression with respect to electronic information in each foreign country. Such assessment shall consist of the following:

''(A) An assessment of the extent to which government authorities in each country inappropriately attempt to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion or belief via the internet, including electronic mail, as well as a description of the means by which such authorities attempt to block or remove such expression.

''(B) An assessment of the extent to which government authorities in each country have persecuted or otherwise punished an individual or group for the nonviolent expression of political, religious, or ideological opinion or belief via the internet, including electronic mail.

''(C) An assessment of the extent to which government authorities in each country have sought to inappropriately collect, request, obtain, or disclose personally identifiable information of a person in connection with such person's nonviolent expression of political, religious, or ideological opinion or belief, including expression that would be protected by the International Covenant on Civil and Political Rights.

''(D) An assessment of the extent to which wire communications and electronic communications are monitored without regard to the principles of privacy, human rights, democracy, and rule of law.

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

''(3) In this subsection—

''(A) the term 'electronic communication' has the meaning given such term in section 2510 of title 18, United States Code;

''(B) the term 'internet' has the meaning given such term in section 231(e)(3) of the Communications Act of 1934 (47 U.S.C. 231(e)(3));

''(C) the term 'personally identifiable information' means data in a form that identifies a particular person; and

''(D) the term 'wire communication' has the meaning given such term in section 2510 of title 18, United States Code.''.

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

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

(2) by adding at the end the following new subsection:

''(k)(1) The report required by subsection (b) shall include an assessment of freedom of expression with respect to electronic information in each foreign country. Such assessment shall consist of the following:

''(A) An assessment of the extent to which government authorities in each country inappropriately attempt to filter, censor, or otherwise block or remove nonviolent expression of political or religious opinion or belief via the internet, including electronic mail, as well as a description of the means by which such authorities attempt to block or remove such expression.

''(B) An assessment of the extent to which government authorities in each country have persecuted or otherwise punished an individual or group for the nonviolent expression of political, religious, or ideological opinion or belief via the internet, including electronic mail.

''(C) An assessment of the extent to which government authorities in each country have sought to inappropriately collect, request, obtain, or disclose personally identifiable information of a person in connection with such person's nonviolent expression of political, religious, or ideological opinion or belief, including expression that would be protected by the International Covenant on Civil and Political Rights.

''(D) An assessment of the extent to which wire communications and electronic communications are monitored without regard to the principles of privacy, human rights, democracy, and rule of law.

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

''(3) In this subsection—

''(A) the term 'electronic communication' has the meaning given such term in section 2510 of title 18, United States Code;

''(B) the term 'internet' has the meaning given such term in section 231(e)(3) of the Communications Act of 1934 (47 U.S.C. 231(e)(3));

''(C) the term 'personally identifiable information' means data in a form that identifies a particular person; and

''(D) the term 'wire communication' has the meaning given such term in section 2510 of title 18, United States Code.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from California (Mr. ROYCE) and the gentleman from New Jersey (Mr. SIRES) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. ROYCE of California. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from California?

There was no objection.

Mr. ROYCE of California. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, let me begin by saying the United States is increasingly under attack by foreign actors online. Nobody knows this better than our members on the Foreign Affairs Committee, but especially MIKE MCCAUL, who assisted me on this bill. As you know, MIKE MCCAUL also chairs the Homeland Security Committee.

So this legislation is focused on correcting a serious threat.

Malicious cyber activities by state and non-state actors threaten our U.S. foreign policy, our security, and our economic interests right now around the globe.

Last year, the intelligence community's Worldwide Threat Assessment summed this up well. As they looked at the problem, they said: ''Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving our cyber defenses, nearly all information, communication networks, and systems will be at risk for years.''

But it is not just the security of our networks that the United States needs to protect. It is the very fabric of the internet itself that is increasingly under assault by governments that want to erect digital borders, that want to impose more control, and that want censorship online.

The State Department has a critical role to play in promoting an open and secure cyberspace by developing international norms of responsible state behavior and deterring malicious actors from carrying out destructive cyber operations.

Last year, the President signed an executive order charging the Secretary of State with creating an interagency strategy to protect the American people from cyber threats along with a plan to improve international cooperation in cybersecurity.

Despite the prominent role assigned to the Department by the President's executive order and support from this body for such work, the office tasked with leading this effort for the State Department was merged into the Bureau of Economic and Business Affairs. The concern is that this limits the Department's ability to confront the full range of issues in cyberspace—such as security, internet access, online human rights, and cybercrime—beyond the clear economic challenges.

So I believe this sends the wrong signal to Moscow, to Beijing, and to other governments around the world. The United States should make it clear that we place a high priority on the whole range of cyber issues, including cybersecurity, internet access, online rights, deterrence, and cybercrime.

In testimony before the Foreign Affairs Committee—and here is the good news—I was relieved to hear our Deputy Secretary Sullivan say that this was just an interim step and that he expects cyber issues will ultimately be elevated to a Senate-confirmed role. This is exactly what this bill requires.

So now, more than ever, we need a high-ranking cyber diplomat at the State Department to prioritize these efforts to ensure that we keep the internet open, keep it reliable, and keep it secure. The bipartisan Cyber Diplomacy Act is going to help counter foreign threats on the internet, it is going to promote human rights abroad, and it is going to also, by the way, create new jobs and economic growth here at home.

Mr. Speaker, I urge my colleagues to support the bill, and I reserve the balance of my time.

Mr. SIRES. Mr. Speaker, I yield myself such time as I may consume.

I rise today in support of this measure.

Mr. Speaker, let me first thank our chairman of the Foreign Affairs Committee, ED ROYCE, and Ranking Member ELIOT ENGEL, for their leadership on this issue.

Mr. Speaker, malicious cyber activity has become a grave threat to the United States and our allies.

In 2014, North Korea hacked Sony Pictures. In 2015, the Chinese stole the personal data of millions of people from the Office of Personnel Management.

In 2016, Russia illegally interfered in our Presidential election, stealing election data and doing real damage to American democracy.

Now, in 2018, our midterm elections are at risk. Putin and his cronies were not finished after the last election. They have hacked our allies, and they will hack our elections again and again unless we do something about it.

We cannot allow foreign governments to meddle in democracy and steal data from our networks. To stand up against these threats, this bill establishes a high-level ambassador to lead the State Department's cyber diplomacy efforts. It also requires the Secretary of State to create an international cyber policy that will improve international cyber norms on security and democratic principles, including a commitment to keep the internet free, open, and interoperable.

America cannot cede cyberspace to China or Russia. Now, more than ever, we need to use all the tools we have to help shape international norms, ramp up coordination with our partners, and stiffen our defenses.

Mr. Speaker, I urge my colleagues to support this bipartisan measure, and I reserve the balance of my time.

Mr. ROYCE of California. Mr. Speaker, I yield 3 minutes to the gentleman from Texas (Mr. MCCAUL), who is the chairman of the Homeland Security Committee.

Mr. MCCAUL. Mr. Speaker, I rise today in support of the Cyber Diplomacy Act, and I want to thank Chairman ROYCE and ELIOT ENGEL for their strong work on this very important issue.

As chairman of the Homeland Security Committee, I have passed numerous bills to strengthen our cyber operations to defend the American people and the homeland. Now, I am pleased to see that we are doing the same at the State Department.

As we have seen, rapid technological advancements have increased our dependence on computer networks. With this growing dependence comes exposure to the myriad vulnerabilities and threats from cybercriminals and hackers but also nation states who continue to launch malicious attacks against us.

Currently, as the chairman stated, there are no real international norms or standards to follow when it comes to cybersecurity. As the threat landscape continues to evolve, I believe that Congress must put forth responsible policies to keep pace—protecting our systems, our critical infrastructure, and American citizens' information and privacy.

This legislation helps ensure the open, reliable, and secure use of the internet by establishing the Office of Cyber Issues within the Department of State, headed by an ambassador responsible for advancing U.S. national security and foreign policy interests on cybersecurity and issues of internet freedom around the globe.

This legislation also requires the Secretary of State to produce a strategy on cyberspace to guide U.S. policy.

Lastly, it requires the State Department to add a section to its annual report on human rights detailing governments'—such as Iran, Russia, and China—silence of their opposition through internet censorship.

Mr. Speaker, I stand proud to be with my colleagues in the House in a bipartisan fashion to propose solutions to these very grave challenges that face the United States and the world.

□ 1430

Mr. SIRES. Mr. Speaker, I yield 4 minutes to the gentleman from Rhode Island (Mr. LANGEVIN), co-chair of the Congressional Cybersecurity Caucus.

Mr. LANGEVIN. Mr. Speaker, I thank the gentleman for yielding.

Mr. Speaker, I rise today in strong support of the Cyber Diplomacy Act and efforts to increase international cooperation and promote global stability in cyberspace.

As the cofounder and co-chair of the Congressional Cybersecurity Caucus, I firmly believe that cybersecurity is the national and economic security challenge of the 21st century, and we must integrate cyberspace into our foreign

policy if we are to successfully mitigate the many threats that we face in this new domain.

Then-Secretary of State Hillary Clinton recognized this when she created the Office of the Cyber Coordinator within the State Department in 2011, and her successor, Secretary John Kerry, continued American leadership in cyber diplomacy.

I had the privilege of working with the inaugural cyber coordinator, Chris Painter, and we are deeply indebted for his 6 years of service in that role. I cannot remember a meeting I had with a cybersecurity expert from a foreign government where his name did not come up as someone who is actively promoting American interest in a free, open, and secure internet.

I am deeply grateful for the leadership of Chairman ROYCE and Ranking Member ENGEL in recognizing the importance of this role and bringing this bill forward to codify and expand it.

This effort is particularly timely as, since Mr. Painter left, there has been some confusion about whether the position would even be filled or if the office would be reorganized under the Bureau of Economic and Business Affairs. It is my goal to see that that does not happen and that this bill prevails. That position deeply needs to be in the State Department, where we can show American leadership on a diplomatic front in cyber.

As a Member who serves on two national security committees, I must emphasize that cybersecurity is not just an economic issue, and this bill appropriately recognizes the broad scope of cyber diplomacy.

Mr. Speaker, every armed conflict going forward in the world today has—and all future conflicts will have—a cyber component. We have seen our cyber adversaries like Russia use cyber tools as instruments of statecraft, including efforts to undermine faith in the bedrock of our democracy, our elections.

We must engage bilaterally and multilaterally with our international partners and even our adversaries in order to protect our interests and allow us to continue to reap the benefits of a connected society.

The lack of policies, norms, and precedents in this new sphere of state interaction continues to increase the potential for a cyber incident to lead to escalating conflict. It is up to the hard-working and, sadly, underappreciated members of our foreign service to change this paradigm and encourage generally stabilizing rules of the road in cyberspace, and this bill will ensure they have the leadership structure to do just that.

Mr. Speaker, let me again thank the chairman and ranking member for their extraordinary work on this important bill.

Mr. ROYCE of California. Mr. Speaker, I continue to reserve the balance of my time.

Mr. SIRES. Mr. Speaker, I yield myself such time as I may consume.

In closing, keeping the internet open, interoperable, and secure is of critical importance to America's national security, economy, and domestic values. We must use all the diplomatic tools to develop strong international norms, bolster our cyber defenses, and promote internet freedom. H.R. 3776 is a necessary step to ensure the United States stays engaged on these critical issues.

Mr. Speaker, I urge my colleagues to support this bill, and I yield back the balance of my time.

Mr. ROYCE of California. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, in closing, I would like to thank Mr. SIRES. I appreciate his efforts in supporting this legislation. I thank Mr. ENGEL and Mr. MCCAUL, as well.

As the birthplace of the internet, it is the United States that has been most impacted. We have a foreign policy and economic interests and have been working internationally to ensure that the internet remains open. Part of our idea is that this would be capable of carrying the free flow of ideas. We thought it should remain reliable and secure.

But increasingly authoritarian regimes are very aggressively promoting a different vision from the one that Americans brought to the table, their vision of cyber sovereignty, which they sometimes call it. What cyber sovereignty means for these governments is state control over cyberspace. That does run counter to the values of a free people and the values of individual and economic liberty.

Working with our allies and partners, I think the United States has got to be prepared to advance our own vision of cyberspace when it is under this kind of attack and censorship. The Cyber Diplomacy Act will give us the tools to do just that.

Mr. Speaker, I thank my colleagues for their help with this legislation, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from California (Mr. ROYCE) that the House suspend the rules and pass the bill, H.R. 3776, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

GLOBAL HEALTH INNOVATION ACT OF 2017

Mr. ROYCE of California. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1660) to direct the Administrator of the United States Agency for International Development to submit to Congress a report on the development and use of global health innovations in the programs, projects, and activities of the Agency.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1660

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Global Health Innovation Act of 2017''.

SEC. 2. ANNUAL REPORT.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter for a period of 4 years, the Administrator of the United States Agency for International Development shall submit to Congress a report on the development and use of global health innovations in the programs, projects, and activities of the Agency.

(b) MATTERS TO BE INCLUDED.—The report required by subsection (a) shall include the following:

(1) A description of—

(A) the extent to which global health innovations described in subsection (a) include drugs, diagnostics, devices, vaccines, electronic and mobile health technologies, and related behavior change and service delivery innovations;

(B) how innovation has advanced the Agency's commitments to achieving an HIV/AIDS-free generation, ending preventable child and maternal deaths, and protecting communities from infectious diseases, as well as furthered by the Global Health Strategic Framework;

(C) how goals are set for health product development in relation to the Agency's health-related goals and how progress and impact are measured towards those goals;

(D) how the Agency's investments in innovation relate to its stated goals; and

(E) progress made towards health product development goals.

(2) How the Agency, both independently and with partners, donors, and public-private partnerships, is—

(A) leveraging United States investments to achieve greater impact in health innovation;

(B) engaging in activities to develop, advance, and introduce affordable, available, and appropriate global health products; and

(C) scaling up appropriate health innovations in the development pipeline.

(3) A description of collaboration and coordination with other Federal departments and agencies, including the Centers for Disease Control and Prevention, in support of global health product development, including a description of how the Agency is working to ensure critical gaps in product development for global health are being filled.

(4) A description of how the Agency is coordinating and aligning global health innovation activities between the Global Development Lab, the Center for Accelerating Innovation and Impact, and the Bureau for Global Health.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from California (Mr. ROYCE) and the gentleman from New Jersey (Mr. SIRES) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. ROYCE of California. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and include any extraneous material on the bill.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from California?