115TH CONGRESS  
1ST SESSION  
H. R. 2812

To direct the President to develop a strategy for the offensive use of cyber capabilities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES  
JUNE 7, 2017

Mr. Correa introduced the following bill; which was referred to the Committee on Foreign Affairs, and in addition to the Committee on Armed 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 direct the President to develop a strategy for the offensive use of cyber capabilities, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the “Enhance Partner Cyber Capabilities Act”.

SEC. 2. FINDINGS.

(1) The North Atlantic Treaty Organization (commonly known as “NATO”) remains a critical alliance for the United States and a cost-effective,
flexible means of providing security to the most im-
portant allies of the United States.

(2) The regime of Russian President Vladimir
Putin is actively working to erode democratic sys-
tems of NATO member states, including the United
States.

(3) According to the report of the Office of the
Director of National Intelligence dated January 6,
2017, on the Russian Federation’s hack of the
United States presidential election: “Russian efforts
to influence the 2016 presidential election represent
the most recent expression of Moscow’s longstanding
desire to undermine the US-led liberal democratic
order.”.

(4) As recently as May 4, 2017, the press re-
ported a massive cyber hack of French President
Emmanuel Macron’s campaign, likely attributable to
Russian actors.

(5) It is in the core interests of the United
States to enhance the offensive and defensive cyber
capabilities of NATO member states to deter and
defend against Russian cyber and influence oper-
ations.

(6) Enhanced offensive cyber capabilities would
enable the United States to demonstrate strength
and deter the Russian Federation from threatening NATO, while reassuring allies, without a provocative buildup of conventional military forces.

**SEC. 3. SENSE OF CONGRESS ON CYBER STRATEGY OF THE DEPARTMENT OF DEFENSE.**

It is the sense of Congress that—

(1) the Secretary of Defense should update the cyber strategy of the Department of Defense (as that strategy is described in the Department of Defense document titled “The Department of Defense Cyber Strategy” dated April 15, 2015);

(2) in updating the cyber strategy of the Department, the Secretary should—

(A) specifically develop an offensive cyber strategy that includes plans for the offensive use of cyber capabilities, including computer network exploitation and computer network attacks, to thwart air, land, or sea attacks by the regime of Russian President Vladimir Putin and other adversaries;

(B) provide guidance on integrating offensive tools into the cyber arsenal of the Department; and

(C) assist NATO partners, through the NATO Cooperative Cyber Center of Excellence
and other entities, in developing offensive cyber capabilities.

SEC. 4. STRATEGY FOR OFFENSIVE USE OF CYBER CAPABILITIES.

(a) STRATEGY REQUIRED.—The President shall develop a written strategy for the offensive use of cyber capabilities by departments and agencies of the Federal Government.

(b) ELEMENTS.—The strategy developed under subsection (a) shall include, at minimum—

(1) a description of enhancements that are needed to improve the offensive cyber capabilities of the United States and partner nations, including NATO member states; and

(2) a statement of principles concerning the appropriate deployment of offensive cyber capabilities.

(c) SUBMISSION TO CONGRESS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the President shall submit to the congressional defense committees (as that term is defined in section 101(a)(16) of title 10, United States Code) the strategy developed under subsection (a).
(2) Form of Submission.—The strategy submitted under paragraph (1) may be submitted in classified form.

SEC. 5. INTERNATIONAL COOPERATION.

(a) Authority To Provide Technical Assistance.—The President, acting through the Secretary of Defense and with the concurrence of the Secretary of State, is authorized to provide technical assistance to NATO member states to assist such states in developing and enhancing offensive cyber capabilities.

(b) Technical Experts.—In providing technical assistance under subsection (a), the President, acting through the NATO Cooperative Cyber Center of Excellence, may detail technical experts in the field of cyber operations to NATO member states.

(e) Rule of Construction.—Nothing in this section shall be construed to preclude or limit the authorities of the President or the Secretary of Defense to provide cyber-related assistance to foreign countries, including the authority of the Secretary to provide such assistance under section 333 of title 10, United States Code.