111TH CONGRESS
2D SESSION

S. 3193

To establish within the office of the Secretary of State a Coordinator for Cyberspace and Cybersecurity Issues.

IN THE SENATE OF THE UNITED STATES

APRIL 12, 2010

Mr. KERRY (for himself and Mrs. GILLIBRAND) introduced the following bill; which was read twice and referred to the Committee on Foreign Relations

---

A BILL

To establish within the office of the Secretary of State a Coordinator for Cyberspace and Cybersecurity Issues.

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 ''International Cyberspace and Cybersecurity Coordination Act of 2010''.

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) On February 2, 2010, Admiral Dennis C. Blair, the Director of National Intelligence, testified before the Select Committee on Intelligence of the

Senate regarding the Annual Threat Assessment of the U.S. Intelligence Community, stating ''The national security of the United States, our economic prosperity, and the daily functioning of our government are dependent on a dynamic public and private information infrastructure, which includes telecommunications, computer networks and systems, and the information residing within. This critical infrastructure is severely threatened. . . . We cannot protect cyberspace without a coordinated and collaborative effort that incorporates both the US private sector and our international partners.''.

(2) In a January 2010 speech on Internet freedom, Secretary of State Hillary Clinton stated: ''Those who disrupt the free flow of information in our society, or any other, pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an Internet-connected world, an attack on one nation's networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons.''.

(3) James Lewis, senior fellow at the Center for Strategic and International Studies asserts, in Securing Cyberspace for the 44th Presidency, ''The international aspects of cybersecurity have been among the least developed elements of U.S. cybersecurity policy. Given the multinational and global aspects of network security, this must be remedied, as energetic engagement could produce real benefits in promoting U.S. objectives and reducing risk.''.

(4) The 2010 National Broadband Plan of the Federal Communications Commission recommends that ''[t]he Executive Branch should develop a coordinated foreign cybersecurity assistance program to assist foreign countries in the development of legal and technical expertise to address cybersecurity.''.

(5) The May 2009 White House Cyberspace Policy Review asserts ''[t]he Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. International norms are critical to establishing a secure and thriving digital infrastructure.''.

SEC. 3. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) even as the United States and the global system have become increasingly more dependent on cyberspace for basic and critical functions and services, a lack of sufficient norms and principles to govern the international cyberspace environment has resulted in significant cyber vulnerabilities and the potential for massive state failure in the event of coordinated cyber attacks;

(2) the multilateral system has not—

(A) addressed these vulnerabilities in a consistent or systematic manner; or

(B) established a basic framework of best practices and governance to address and respond to emerging cyber threats;

(3) the international community should strongly consider the utility of negotiating a multilateral framework on cyberwarfare that would create shared norms for cyber conduct and head off the potentiality for larger disruptions related to cyberwarfare;

(4) United States diplomatic engagement towards international cybersecurity issues—

(A) has been uncoordinated and fragmented; and

(B) has not taken advantage of securing cyberspace within a multilateral framework;

(5) the Secretary of State, in consultation with other relevant Federal agencies, should develop and establish a clear and coordinated strategy for international cyberspace and cybersecurity engagement, which should—

(A) review and assess existing strategies for international cyberspace and cybersecurity policy and engagement;

(B) define short- and long-term objectives for United States cyberspace and cybersecurity policy;

(C) consider how to support a policy of United States Government collaboration and coordination with other countries and organizations in order to bolster an international framework of cyber norms, governance, and deterrence;

(D) consider the utility of negotiating a multilateral framework that would provide internationally acceptable principles to better mitigate cyberwarfare, including noncombatants;

(E) share and disseminate relevant threat information with key stakeholders;

(F) be developed in consultation with other United States Government agencies with relevant technical expertise or policy mandates pertaining to cyberspace and cybersecurity issues; and

(G) draw upon the expertise of technology, security, and policy experts, private sector actors, international organizations, and other appropriate entities.

SEC. 4. COORDINATOR FOR CYBERSPACE AND CYBERSECURITY ISSUES.

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

(1) in subsection (e), by striking ''in this paragraph referred to'' and inserting ''referred to in this subsection'';

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

(3) by inserting after subsection (f) the following:

''(g) CYBERSPACE AND CYBERSECURITY ISSUES.—

''(1) IN GENERAL.—There is established within the office of the Secretary of State a Coordinator for

Cyberspace and Cybersecurity Issues (referred to in this subsection as the 'Coordinator'), who shall be appointed by the President, by and with the advice and consent of the Senate.

''(2) DUTIES.—

''(A) PRINCIPAL DUTIES.—The Coordinator shall—

''(i) be the principal official within the senior management of the Department of State responsible for cyberspace and cybersecurity issues;

''(ii) be the principal advisor to the Secretary of State on international cyberspace and cybersecurity issues;

''(iii) report directly to the Secretary of State; and

''(iv) perform such duties and exercise such powers as the Secretary of State shall prescribe.

''(B) ADDITIONAL DUTIES.—In addition to the duties described in subparagraph (A), the Coordinator shall—

''(i) provide strategic direction and coordination for United States Government policy and programs aimed at addressing

and responding to cyberspace and cybersecurity issues overseas, especially in relation to issues that affect United States foreign policy and related national security concerns;

''(ii) coordinate with relevant Federal departments and agencies, including the Department of Homeland Security, the Department of Defense, the Department of the Treasury, the Department of Justice, the Department of Commerce, and the intelligence community to develop interagency plans regarding international cyberspace and cybersecurity issues;

''(iii) provide a focal point for the private sector to coordinate on international cyberspace and cybersecurity issues; and

''(iv) build multilateral cooperation to develop international norms, common policies, and responses to secure the integrity of cyberspace.

''(3) RANK AND STATUS OF AMBASSADOR.—The Coordinator shall have the rank and status of Ambassador at Large.

''(4) COUNTRY AND REGIONAL CYBERSPACE AND CYBERSECURITY POLICY COORDINATORS.—The Secretary of State, in consultation with the heads of other relevant Federal agencies and in coordination with the relevant Chief of Mission, should designate an employee to have primary responsibility for matters relating to cyberspace and cybersecurity policy in each country or region that the Secretary considers significant with respect to efforts of the United States Government to combat cybersecurity globally.''.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to carry out this Act and the amendments made by this Act.

○