116TH CONGRESS
1ST SESSION

S. RES. 140

Urging the establishment of a Cyber League of Indo-Pacific States to address cyber threats.

IN THE SENATE OF THE UNITED STATES

APRIL 3, 2019

Mr. GARDNER (for himself and Mr. COONS) submitted the following resolution; which was referred to the Committee on Foreign Relations

---

RESOLUTION

Urging the establishment of a Cyber League of Indo-Pacific States to address cyber threats.

Whereas the world has benefitted greatly from technological innovations under the leadership of the United States in the post-World War era, including the creation of the World Wide Web which has provided an entirely new platform for wealth creation and human flourishing through cyber-commerce and connectivity;

Whereas cybercrime affects companies large and small, as well as infrastructure that is vital to the economy as a whole;

Whereas a 2018 study from the Center for Strategic and International Studies, in partnership with McAfee, estimates that the global economic losses from cybercrime are approximately $600,000,000,000 annually and rising;

Whereas, according to the Pew Charitable Trust, 64 percent of people in the United States had fallen victim to cybercriminals as of 2017;

Whereas, on July 9, 2012, General Keith Alexander, then-Director of the National Security Agency, termed theft of United States intellectual property ''the greatest transfer of wealth in history'';

Whereas, on September 25, 2015, the United States and the People's Republic of 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'';

Whereas the People's Republic of China nonetheless continues to contribute to the rise of cybercrime, exploiting weaknesses in the international system to undermine fair competition in technology and cyberspace, including through theft of intellectual property and state-sponsored malicious actions to undermine and weaken competition;

Whereas, according to the 2019 Worldwide Threat Assessment by the Director of National Intelligence: ''China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.'';

Whereas, from 2011 to 2018, more than 90 percent of cases handled by the Department of Justice alleging economic espionage by or to benefit a foreign country involved the People's Republic of China;

Whereas more than ⅔ of the cases handled by the Department of Justice involving theft of trade secrets have a nexus to the People's Republic of China;

Whereas experts have asserted that the Made in China 2025 strategy of the Government of the People's Republic of China will incentivize Chinese entities to engage in unfair competitive behavior, including additional theft of technologies and intellectual property;

Whereas the Democratic People's Republic of Korea has also contributed to the rise of cybercrime and according to the 2018 Worldwide Threat Assessment by the Director of National Intelligence: ''We expect the heavily sanctioned North Korea to use cyber operations to raise funds and to gather intelligence or launch attacks on South Korea and the United States. . . . North Korean actors developed and launched the WannaCry ransomware in May 2017, judging from technical links to previously identified North Korean cyber tools, tradecraft, and operational infrastructure. We also assess that these actors conducted the cyber theft of $81 million from the Bank of Bangladesh in 2016.'';

Whereas section 2(a)(8) of the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. 9201(a)(8)) states, ''The Government of North Korea has provided technical support and conducted destructive and coercive cyberattacks, including against Sony Pictures Entertainment and other United States persons.'';

Whereas the United States has taken action on its own against international cybercrime, including through—

(1) the North Korea Sanctions and Policy Enhancement Act of 2016 (Public Law 114–122), which imposed mandatory sanctions against persons engaging in signifi-

cant activities undermining cybersecurity on behalf of the Democratic People's Republic of Korea; and

(2) criminal charges filed by the Department of Justice on October 25, 2018, in which the Department alleged that the Chinese intelligence services conducted cyber intrusions against at least a dozen companies in order to obtain information on a commercial jet engine;

Whereas 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'';

Whereas concerted action by countries that share concerns about state-sponsored cyber theft is necessary to prevent the growth of cybercrime and other destabilizing national security and economic outcomes; and

Whereas section 215 of the Asia Reassurance Initiative Act of 2018 (Public Law 115–409) calls for ''robust cybersecurity cooperation between the United States and nations in the Indo-Pacific region'' and ''authorized to be appropriated $100,000,000 for each of the fiscal years 2019 through 2023 to enhance cooperation between the United States and the Indo-Pacific nations for the purpose of combatting cybersecurity threats'': Now, therefore, be it

Resolved, That the Senate—

(1) urges the President to propose and champion the negotiation of a treaty with like-minded partners in the Indo-Pacific to ensure a free and open Internet free from economically crippling cyberattacks;

(2) calls for the treaty, which can be referred to as the Cyber League of Indo-Pacific States (in this resolution referred to as ''CLIPS''), to include the creation of an Information Sharing Analysis Center to provide around-the-clock cyber threat monitoring and mitigation for governments that are parties to the treaty; and

(3) calls for members of CLIPS—

(A) to consult on emerging cyber threats;

(B) to pledge not to conduct or support theft of intellectual property, including trade secrets or other confidential business information;

(C) to introduce and enforce minimum criminal punishment for cyber theft;

(D) to extradite alleged cyber thieves, consistent with existing agreements and respecting national sovereignty;

(E) to enforce laws protecting intellectual property, including patents;

(F) to ensure that government agencies comply with software license terms;

(G) to minimize data localization requirements (consistent with the Agreement between the United States of America, the United Mexican States, and Canada, signed at Buenos

Aires November 30, 2018 (commonly known as the ''United States-Mexico-Canada Agreement'');

(H) to seek cooperation with respect to the standards described in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, dated May 14, 2014;

(I) to provide for public input when devising legislation on cybersecurity; and

(J) to cooperate on the attribution of cyberattacks and impose appropriate consequences.

○