113TH CONGRESS
2D SESSION

H. RES. 643

Calling for further defense against the People's Republic of China's state-sponsored cyber-enabled theft of trade secrets, including by the People's Liberation Army.

IN THE HOUSE OF REPRESENTATIVES

JUNE 25, 2014

Mr. CHABOT (for himself, Mr. BERA of California, Mr. COHEN, Mr. COLLINS of Georgia, and Mr. CONNOLLY) submitted the following resolution; which was referred to the Committee on the Judiciary, and in addition to the Select Committee on Intelligence (Permanent Select), Armed Services, Ways and Means, and Foreign Affairs, 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

---

RESOLUTION

Calling for further defense against the People's Republic of China's state-sponsored cyber-enabled theft of trade secrets, including by the People's Liberation Army.

Whereas the People's Republic of China (PRC) has been labeled by the United States Office of the National Counterintelligence Executive as the world's most active and persistent perpetrator of economic espionage;

Whereas the Permanent Select Committee on Intelligence of the House of Representatives investigated the PRC's major telecommunications companies and concluded in a bipartisan report released October 2012 that Chinese

businesses Huawei Technologies' and ZTE Incorporated's provision of equipment to United States critical infrastructure could undermine core United States national security interests;

Whereas in February 2013, the President issued the Administration's Strategy on Mitigating the Theft of United States Trade Secrets and stated, ''We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and economy.'';

Whereas Mandiant, a United States cybersecurity firm, reported in February 2013 that a cyber-hacking group it labels as Advanced Persistent Threat 1 (APT1) is based in the PRC and is likely government-sponsored;

Whereas Mandiant found that APT1 is known as Unit 61398 and is the 2nd Bureau of the 3rd Department of the General Staff Department of the People's Liberation Army (PLA) under the Communist Party of China;

Whereas Mandiant warned that APT1 is only one of more than 20 Advanced Persistent Threat groups originating in the PRC;

Whereas Mandiant concluded that APT1 has conducted a cyber espionage campaign since at least 2006, whereas since that time, APT1 systematically stole hundreds of terabytes of data from at least 141 companies in 20 major industries;

Whereas Mandiant detailed that APT1 focuses on compromising organizations in a broad range of industries in English-speaking countries and maintains an extensive infrastructure of computer systems around the world;

Whereas Director of National Intelligence James Clapper reported to Congress in March 2013 that the PRC remains

one of the most capable and persistent intelligence threats;

Whereas in May 2013, the Secretary of Defense reported to Congress in a report entitled ''Military and Security Developments Involving the People's Republic of China'' that in 2012, numerous computer systems around the world, including those owned by the United States Government, were targeted for intrusions, some of which were attributable directly to the Government and military of the PRC;

Whereas the Secretary of Defense asserted that these intrusions carried out by the PRC were focused on exfiltrating information through computer network exploitation (CNE) capabilities to support state-sponsored intelligence collection of United States national defense programs;

Whereas Director of National Intelligence James Clapper reported to Congress in January 2014 that China seeks to revise the multi-stakeholder model of Internet governance while continuing its expansive worldwide program of network exploitation and intellectual property theft;

Whereas Attorney General Eric Holder announced on May 19, 2014, an indictment against five hackers affiliated with the PLA for serious cyber economic espionage that victimized United States entities and stole trade secrets;

Whereas these five hackers were identified as part of Unit 61398 of the PLA;

Whereas the indictment detailed the threat from Unit 61398 of the PLA based in Shanghai in the PRC; and

Whereas this indictment was the first time charges were brought against state actors for cyber infiltration of United States commercial entities: Now, therefore, be it;

Resolved, That the House of Representatives—

(1) calls on the President to aggressively implement and coordinate the Strategy on Mitigating the Theft of United States Trade Secrets;

(2) calls on the PRC to end the practice of cyber-enabled espionage against United States firms and individuals and to cooperate in cyber security efforts with the United States;

(3) calls on the Department of Justice to continue to advance investigations into cyber espionage by actors originating in the PRC;

(4) calls on the United States Government to continue to condemn cyber-enabled espionage for the purposes of stealing intellectual property and trade secrets, pursue counter intelligence capacities, and prosecute such individuals should they enter United States territory;

(5) calls on the United States Trade Representative to estimate the loss from cyber theft, compile a list of actors that cause the most damage to United States firms by intellectual property rights theft and pursue a dispute settlement case at the World Trade Organization;

(6) calls on the United States Office of the National Counterintelligence Executive to update the

unclassified report to Congress on Foreign Economic Collection and Industrial Espionage in 2009–2011 with information that includes the cyber threat from the People's Republic of China against United States companies and critical infrastructure;

(7) calls on the Department of Defense to restrict military-to-military contacts with the PLA in compliance with United States laws, including the National Defense Authorization Act for Fiscal Year 2000 (Public Law 106–65);

(8) calls on the Federal Bureau of Investigation and the Department of Homeland Security to expand warnings to United States companies about the broad scope of tools to illicit trade secrets used by actors originating in the PRC, including cyber theft, physical trespass of the factories or other facilities of United States firms, intrusion of computers, and use of Universal Serial Bus (USB) drives, money, travel, gifts, promises of employment, and social media;

(9) calls on the Department of Defense and the Department of State to provide briefings of the United States-China cyber-security working group meetings in 2013; and

(10) calls on Federal departments and agencies to expand cooperation with allies and partners to better coordinate defense against cyber threats.

○