116TH CONGRESS
2D SESSION

H. RES. 827

Affirming that all Chinese companies, private and state-owned, are under the effective control of the Chinese Communist Party.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 3, 2020

Mr. MCCAUL (for himself, Ms. CHENEY, Mr. TURNER, Mr. GALLAGHER, and Mr. YOHO) submitted the following resolution; which was referred to the Committee on Foreign Affairs

---

RESOLUTION

Affirming that all Chinese companies, private and state-owned, are under the effective control of the Chinese Communist Party.

Whereas the United States and the United Kingdom have a special relationship and shared history of fighting totalitarianism and communism regardless of cost;

Whereas the decision by the British National Security Council to allow Huawei into its fifth-generation (5G) telecommunication network is deeply concerning to the United States;

Whereas banning Huawei from ''sensitive parts'' of the network, known as the core, and capping Huawei's market share at 35 percent is not enough to ensure the security and fidelity of the United Kingdom's 5G network;

Whereas in order to realize the full potential of 5G, there will be no means to isolate one part of the network from other components; therefore, granting an untrusted provider access to any portion of the network inevitably risks opening access to the entire network, including the ability to take the entire network offline and deny the United Kingdom strategically important services;

Whereas the United Kingdom's Telecom Supply Chain Review requires the United Kingdom to consider, with respect to a high-risk vendor such as Huawei, the ''domestic security laws in the jurisdiction where the vendor is based. . . .'';

Whereas the political economy and laws and regulations of the People's Republic of China (PRC) are an affront to the democratic values shared by the United States and the United Kingdom;

Whereas under the leadership of General Secretary Xi Jinping, the unelected Chinese Communist Party (CCP) leads everything;

Whereas, according to the Fourth Plenum Decision Document, the CCP aims to ''perfect the Party leadership over the National People's Congress, government, supervision organs, trial organs, inspection organs, armed forces, people groups, companies and institutions, grass roots organizations, and social groups.'';

Whereas the CCP oversees the economic and technology policies of the People's Republic of China, directs all legal and regulatory authorities, and exerts direct and indirect influence over all companies in the PRC—state-owned and private;

Whereas the CCP has codified into law its authority to interfere in and influence the operations of companies operating within and outside of the PRC and demand access to any data stored in or transiting through its network equipment;

Whereas Article 30 of the CCP Constitution requires a CCP cell to be formed in any company where there are three of more CCP members;

Whereas Article 15 of Regulations of the CCP on the Work of Grassroots Organizations in State Owned Enterprise requires all important operating and management issues to be discussed by the Party Committee, and only after be decided on by the board of directors or management;

Whereas Article 19 of China's Company Law requires every company to establish a CCP cell and carry out CCP activities and to provide necessary conditions for CCP cell activities;

Whereas Article 26 of the Guideline on Improving Business Conditions for Private Enterprises calls on private businesses to support Party construction;

Whereas, in addition to inserting itself directly into company operations through CCP cells and ownership stakes, the CCP is erecting a legal and regulatory system that in effect gives it direct influence over a company's operations and access to all its personal and business information, thereby turning nominally private companies into resources for and tools of the CCP;

Whereas the PRC's National Security Law declares nearly any issue—from the economy to technology and information to ideology—a matter of national security and intelligence work;

Whereas the PRC's Cybersecurity Law gives the CCP expansive powers over how information technology products are approved and where data and information are stored, including—

(1) Articles 22 and 23 which require network products and services to adhere to mandatory national standards and obtain certain certifications, many of which require the disclosure of proprietary information, such as source code, and the use of indigenously innovated Chinese intellectual property;

(2) Article 28 which mandates any network operator to provide technical support and assistance to public security and national security organs; and

(3) Article 37 which sets forth broad requirements for data and information to be stored within the boundaries of the PRC;

Whereas the National Intelligence Law gives Chinese intelligence agencies authority to compel private companies to support intelligence operations, including Article 7, which requires an organization or citizen to support, assist, and cooperate with state intelligence work, and Article 14, which demands that organizations provide support, assistance, and cooperation to intelligence organs;

Whereas Article 22 of China's Counterespionage Law states that when agencies are investigating espionage activities and collecting evidence, organizations and individuals must not refuse to provide it information;

Whereas Article 18 of the Anti-Terrorism Law states that telecommunications business operators and internet service providers shall provide technical interfaces, decryption, and other technical support and assistance for public security organs and state security organs to prevent

and investigate terrorist activities in accordance with the law;

Whereas Article 31 of the Encryption Law provides for government inspections of commercial encryption that, when used in concert with other laws and regulations, could result in full access of encrypted servers and decryption keys by the CCP;

Whereas several provisions in the Ministry of Public Security Regulation on Internet Security Supervision and Inspection give security organs the right to conduct onsite and remote inspections of company networks—including technical aspects of its operations and the data and information stored on its servers—and allows authorities to copy any information on corporate servers;

Whereas these and other laws, regulations, and standards combined with the Internet+ initiative, the social credit system for individuals and companies, and other industrial and sector-specific plans form the foundation for the PRC's authoritarian digital governance model that it is aggressively exporting around the world;

Whereas the PRC's authoritarian model puts absolute control of the digital economy, including its hardware, software, algorithms, encryption, data, and other proprietary information, into the hands of the CCP, removing any semblance of privacy; and

Whereas General Secretary Xi Jinping has said ''high-end technology is the weapon of a modern country'' and the CCP has clearly demonstrated its ambition to attack global markets with its products and services to make the world safe for its authoritarian model and dependent on its technologies: Now, therefore, be it

Resolved, That it is the sense of the House of Representatives that—

(1) the Parliament of the United Kingdom of Great Britain and Northern Ireland is encouraged to reject or amend the National Security Council's decision on telecommunications security in a manner that excludes high-risk vendors, such as Huawei, from the country's 5G infrastructure;

(2) Huawei's track-record of illegal and corrupt behavior is endemic to their operations;

(3) whether state-owned or nominally private, all Chinese companies, including Huawei, operate within a political and regulatory environment that removes their ability to act independently from or to refuse requests by the CCP;

(4) this distinct state-led economy and communist political system removes independent corporate governance and obscures the true nature of Chinese corporate entities, harming the transparency needed to maintain the international rules-based system;

(5) fifth-generation telecommunications networks that incorporate products and services developed by Chinese companies face significant technological, political, ethical, and geopolitical risk; and

(6) the United States Government and its allies and partners must work expeditiously to develop and implement a concerted strategy, using all tools available, to combat what amounts to legal warfare by the Chinese government to weaponize its companies when needed.

○