

# Congress of the United States

Washington, DC 20515

September 13, 2012

Mr. Frank M. Conner III  
Managing Partner, DLA Piper  
500 Eighth Street, NW  
Washington, D.C. 20004

Mr. Richard Newcomb  
Partner, DLA Piper  
500 Eighth Street, NW  
Washington, D.C. 20004

Dear Mr. Conner and Mr. Newcomb:

We write to express our disappointment with DLA Piper's decision to represent, and subsequently advise and counsel, the Chinese state-owned telecommunications company ZTE Corporation as it attempts to circumvent U.S. government concerns and gain a larger share of the U.S. marketplace.

As you know, the American marketplace is built on openness, transparency in operations, and the separation of government and industry. By contrast, China's version of capitalism is heavily state-dominated, and companies in China do not operate in a private sector that is similar to that in the United States. For example, the telecommunications industry in China has been listed by the government as one of its top "strategic" industries – meaning that "the state must maintain 'absolute control through dominant state-owned enterprises.'<sup>1</sup>" As a state-owned entity within a strategic industry, the ZTE Corporation is subject to unilateral government control, and it is beholden to Chinese national and strategic interests.

The Chinese governing structure allows for little distinction between the government and its military component, the People's Liberation Army (PLA). Moreover, the U.S. Department of Defense (DOD) has confirmed, in an open-source capacity, that the ZTE Corporation maintains close ties to the PLA. DOD specifically references ZTE's ties to the PLA in its 2011 and 2012 open-source security reports to Congress on Chinese military activities.<sup>2,3</sup> This apparent connection between ZTE and the PLA poses a serious problem for the United States, as it is well-documented that Chinese actors – who are often government-sponsored – are among the world's most active in implementing cyber-warfare.

The Defense Department confirms, in open-source, that the Chinese government continues to support frequent cyber-intrusions and data theft operations that target entities within the United States:

Authoritative writings and China's persistent cyber intrusions indicate the likelihood that Beijing is using cyber network operations as a tool to collect strategic intelligence. [...] Chinese actors are the world's most active and persistent perpetrators of economic espionage.

---

<sup>1</sup> U.S.-China Economic and Security Review Commission. "2011 Report to Congress." Page 48. (See: [http://www.uscc.gov/annual\\_report/2011/annual\\_report\\_full\\_11.pdf](http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf)).

<sup>2</sup> U.S. Department of Defense. "Military and Security Developments Involving the People's Republic of China 2011." Page 42. (See: [http://www.defense.gov/pubs/pdfs/2011\\_cmpr\\_final.pdf](http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf)).

<sup>3</sup> U.S. Department of Defense. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012." Page 10. (See: [http://www.defense.gov/pubs/pdfs/2012\\_CMPR\\_Final.pdf](http://www.defense.gov/pubs/pdfs/2012_CMPR_Final.pdf)).

Chinese attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to U.S. economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment.<sup>4</sup>

As a telecommunications company, it is ZTE's business to manufacture and distribute equipment that helps manage, distribute, and store vast quantities of private data. With that in mind, it would be irresponsible for the federal government to ignore China's role in international cyber-espionage and the inherent security risks that are present when a Chinese government-owned company intends to sell information technology products in the American marketplace – including to potential buyers such as the U.S. government, state and local entities, law enforcement officials, critical infrastructure partners, businesses, and private citizens.

In addition to cyber-security and supply chain security concerns, it is equally as troubling that the ZTE Corporation appears to have violated U.S. sanctions on Iran by reportedly providing the Telecommunications Company of Iran (TCI), an Iranian government-controlled entity, with surveillance technologies that would allow TCI the ability to monitor all mobile, landline, and Internet communications that occur throughout Iran.<sup>5</sup> Reports also indicate that ZTE conspired to violate additional export control laws by agreeing to a contract that would have sold embargoed U.S. computer equipment to TCI.<sup>6</sup>

If these reports are accurate, ZTE's actions directly assist the Iranian government's efforts to use technology to further oppress political dissidents and restrict freedom of speech and the free-flow of information in Iran. The Iranian regime's brutal repression affects all Iranians, but it especially targets women's rights organizations, religious minorities, journalists, and student groups.

In case you were not aware, the United Nations' Special Rapporteur on the situation of human rights in Iran, Ahmed Shaheed, offered the following assessment in May 2012 on the condition in Iran:

The conviction and extremely harsh sentencing of human rights defenders is an indication of mounting repression against the legitimate activities of human rights defenders and represents a serious setback for the protection of human rights in Iran.<sup>7</sup>

Both the U.S. Department of Commerce and the Federal Bureau of Investigation (FBI) are investigating ZTE's actions and business in Iran. The FBI is also investigating ZTE's reported intentions to undermine Commerce Department officials – ZTE officials allegedly

---

<sup>4</sup> U.S. Department of Defense. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012." Pages 9-10. (See: [http://www.defense.gov/pubs/pdfs/2012\\_CMPR\\_Final.pdf](http://www.defense.gov/pubs/pdfs/2012_CMPR_Final.pdf)).

<sup>5</sup> Steve Stecklow. "Chinese firm helps Iran spy on citizens." *Reuters*. March 22, 2012. (See: <http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322>).

<sup>6</sup> *Ibid.* "China's ZTE planned U.S. computer sale to Iran." *Reuters*. April 10, 2012. (See: <http://www.reuters.com/article/2012/04/10/us-zte-iran-aryacell-idUSBRE8390T720120410>).

<sup>7</sup> Ahmed Shaheed. U.N. Special Rapporteur on the situation of human rights in Iran. "Independent UN experts urge Iran to ensure protection for rights defenders." (See: <http://www.un.org/apps/news/story.asp?NewsID=41918&Cr=Iran&Cr1=Human%20Rights#.UEkHH7IiYWI>).

conspired to shred documents and alter packing lists in an effort to mislead the U.S. government on its dealings in Iran.<sup>8</sup>

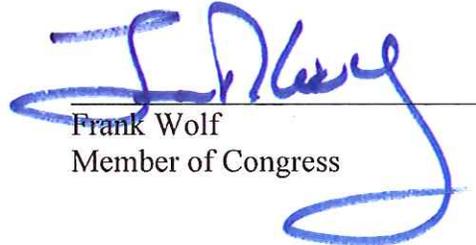
The federal government takes sanctions violations seriously. Given Mr. Newcomb's tenure as the Director of the Treasury Department's Office of Foreign Assets Control (OFAC), we hope that DLA Piper would appreciate the importance of the federal government's ability to enforce the sanctions that Congress legislates. Economic sanctions are, of course, a significant diplomatic tool that the United States can use to leverage the actions of some of the world's most oppressive regimes. ZTE's reported actions run counter to the very efforts that OFAC seeks to enforce.

By publically representing and advising the ZTE Corporation, your firm is indicating that it values the retainer of one contract over the legitimate cyber-security and supply chain concerns of the United States government, as well as the oppression and persecution of political dissidents, human rights advocates, religious groups, women, journalists, students, and educators in Iran. Especially in light of the House Intelligence Committee's hearing this week – as well as its ongoing investigation – on the threats your client may pose to the national security of the United States, we would urge your firm to reconsider its relationship with the ZTE Corporation.

Sincerely,



Sue Myrick  
Member of Congress



Frank Wolf  
Member of Congress

---

<sup>8</sup> Steve Stecklow. "FBI probes China's ZTE over Iran tech deals: report." *Reuters*. (See: <http://www.reuters.com/article/2012/07/13/us-zte-fbi-idUSBRE86C00S20120713>).